ENABLING TECHNIQUES FOR NEXT GENERATION SECURE UNDERWATER OPTICAL COMMUNICATIONS

A Dissertation

by

Burak Kebapci

Submitted to the
Graduate School of Sciences and Engineering
In Partial Fulfillment of the Requirements for
the Degree of

Doctor of Philoshopy

in the
Department of Electrical and Electronics Engineering

Özyeğin University
August 2023

Copyright © 2023 by Burak Kebapci

ENABLING TECHNIQUES FOR NEXT GENERATION SECURE UNDERWATER OPTICAL COMMUNICATIONS

Approved by:

Professor Murat Uysal, Advisor
Department of Electrical and
Electronics Engineering
Özyeğin University

Assistant Professor Vecdi Emre Levent
Department of Computer Engineering
Fenerbahçe University

Assistant Professor Kadir Durak
Department of Electrical and
Electronics Engineering
Özyeğin University

Associate Professor Eylem Erdoğan
Department of Electrical and
Electronics Engineering
Istanbul Medeniyet University

Date Approved: 7 July 2023

Assistant Professor Cagatay Edemen
Department of Electrical and
Electronics Engineering
Özyeğin University

To my Family

ABSTRACT

As threats in the maritime domain diversify, securing data transmission becomes critical for underwater wireless networks designed for the surveillance of critical infrastructure and maritime border protection. This has sparked interest in underwater Quantum Key Distribution (QKD). In this study, a fully functional BB84 QKD system is developed as a solution to emerging security need of underwater wireless communication systems. The QKD unit is built on a hybrid computation system consisting of an Field Programmable Gate Array (FPGA) and an on-board computer (OBC) interfaced with optical front-ends. A real-time photon counting module is implemented on FPGA. The transmitter and receiver units are powered with external UPS and all system parameters can be monitored from the connected computers. The system is equipped with a visible laser and an alignment indicator to validate successful manual alignment. Secure key distribution at a rate of 100 qubits per second was successfully tested over a link distance of 7 meters.

ÖZETÇE

Denizcilik alanındaki tehditler çeşitlenmekte, kritik altyapının gözetimi ve deniz sınırı koruması için tasarlanmış su altı kablosuz ağlar için veri iletiminin güvenliğini sağlamak kritik hale gelmektedir. Bu, su altı Kuantum Anahtar Dağıtımına (QKD) olan ilgiyi günden güne arttırmaktadır. Bu tezde, su altı kablosuz haberleşme sistemlerinin artan güvenlik ihtiyacına bir çözüm olarak tamamen işlevsel bir BB84 QKD sistemi önerilmiştir. QKD birimi, bir FPGA'dan ve optik ön yüzlere arayüzlenmiş yerleşik bir bilgisayardan (OBC) oluşan hibrit bir hesaplama sistemi üzerine kuruludur. FPGA tabanlı gerçek zamanlı bir foton sayma modülü tasarlanmıştır. Verici ve alıcı üniteler harici UPS ile beslenmektedir ve tüm sistem parametreleri bağlı bilgisayarlardan izlenebilmektedir. Sistem, başarılı manuel hizalamayı doğrulamak için görünür bir lazer ve bir hizalama göstergesi ile donatılmıştır. Saniyede 100 kübit hızında güvenli anahtar dağıtımı, 7 metrelik bir bağlantı mesafesinde başarıyla test edilmiştir.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Prof. Dr. Murat Uysal for his remarkable mentorship, guidance, and unwavering support. The impact he has had on my personal and professional growth is immeasurable. I will never forget his support and the many opportunities he provided. I express my sincere gratitude to the esteemed members of my dissertation committee; Assist. Prof. Kadir Durak, Assist. Prof. Cağatay Edemen, Assist. Prof. Vecdi Emre Levent, and Assoc. Prof. Dr. Eylem Erdoğan, for their invaluable time and meticulous review of my dissertation.

Moreover, colleagues from The Center of Excellence for Optical Wireless Communications Technologies (OKATEM) also provided great support on performing hardest experiments. Specially support from Gorkem Mutlu, Ibrahim Baglica, Anilcan Tosun was essential.

I would also like to acknowledge the unwavering support of my family throughout my thesis journey. Their encouragement, understanding, and belief in my abilities have been a constant source of strength and motivation. Their presence and understanding during the ups and downs of this demanding process have been invaluable. I am deeply grateful for their sacrifices, patience, and belief in my abilities. Their support has provided me with the necessary foundation to overcome challenges, persevere, and achieve my goals. I am truly blessed to have such a loving and supportive family. It would not have been possible without the unwavering support of both my Mother Nurten and Father Muhsin. My lovely wife Beyza also performed extraordinary support in the last phases of my thesis. With the great support of my wife, I feel I am ready to overcome biggest challenges in future.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.1 Overview of Underwater Wireless Communication

The first underwater wireless communication experiments were conducted using ultra-low frequencies (ELFs) in the 20th century. Water is extremely absorptive for Radio Frequency (RF) signals, for this reason signal transmission generally limited to few meters. The roots of modern underwater wireless communication go back to World War 2. During World War 2 thousands of submarines were built and operated, and underwater wireless communication became an absolute necessity in complex operations. The first long range underwater telephone was developed by the US Naval Underwater Sound Laboratory Base at 1945 [1]. The system used acoustic transducers operating at 8.3kHz. The state of the art long range acoustic systems can operate even beyond 1000km [2]. The available bandwidth for underwater acoustic communications is limited due to severe attenuation and multi path effects in the underwater channel [3] [4] [5]. Although there are some other alternatives such as MI(Magnetic Induction)[6] [7] and RF [8], underwater optical wireless communication(UOWC) outstands others in terms of the maximum achievable data rates. The electrical signal is transferred to the optical system using lasers or LEDs, and the signal is measured by photodiodes. The UOWC communication systems have been demonstrated to operate reliably even more than 100 meter communication distances [9]. There are already commercial products available such as [10] for long range underwater optical wireless communication. The first example of UOWC experiment is conducted using green laser, achieved 9m link range and 50Mbps data rate at 1992. [11]. The current state of the art UOWC systems are enabled very high datarates in

underwater wireless communications exceeding 100Gbps. [12]

The underwater optical signal transmission works best at visible optical spectrum range as a result of much lower attenuation compared to other wavelengths [13]. The absorption in the underwater signal transmission spectrum is shared in [13]. The blue and green wavelengths specially stand out compared to other wavelengths. This information is valid for most of the cases, but there are some exceptions to that such as in turbid waters, the red wavelengths outperform other wavelengths. [14] The wavelength-dependent optical performance of the signal transmission differs slightly depending on chlorophyll concentration, particle size, and water turbidity.

1.2 Security Aspects of Underwater Wireless Communication

The increased number of deployment of Underwater Sensor Nodes, Remotely Operated Vehicles (ROVs), Autonomous Underwater Vehicles (AUVs), Submarines require instantaneous data transmission [15] and data rate requirement also varies case to case. Although some underwater wireless sensor networks require very simple data transmission between them such as simple water quality measurements in area it is deployed, some underwater surveillance systems might need to share camera or sonar data measurements. Today, underwater wireless sensor networks are actively used in various civil and military purposes. Underwater acoustic communication used for very long-range data transmission that can reach hundreds of kilometers and therefore they are easily tapped by eavesdroppers [16]. On the other hand, the signal travels at relatively low speeds and channel conditions create high amount of doppler effect, which can make the system vulnerable to various cyber attacks such as man-in-the-middle attack, injection attack, etc. [17] [18]. The man in middle attack is basically a eavesdropper stays in middle of the transmit and receive nodes and it listens and tries to manipulate communication. Injection attack is an attacker waits silently for transmitter node to transmit such frames that an attacker can inject faulty information

that receiver will take it and use it. The attacker transmits faulty data and overrides the actual transmitters transmission, since the channel is very lossy and multi path is getting more dominant in long ranges attacker can take advantage of channel conditions. Thus, slow rates and low speed of signal transmission make underwater acoustic communications susceptible to various types of attacks. On the other hand, there are also other physical layer protections such as frequency hoping spread spectrum techniques where transmitter continuously switches between frequencies to prevent jamming of communication line. [19]

The UOWC generally considered to be safer than acoustic communication systems, because they generally use highly directed transmitter and receivers and it operates in relatively short range communication ranges compared to acoustic counterparts. Optical wireless communication systems are inherently safer, still the signal can be tapped with highly sensitive detectors and telescope systems that can add very high gain on receiver [20]. Although the receiver and transmitters are highly directive, the small particles in water are creating scattering on transmitted beam and it redirects some of the photons to go in random directions. On the other hand UOWC systems are also a potential communication solution for air to water or water to air communications [21],[22]. In that case signal can also be tapped by directing a receiver telescope to the beam where the optical signal crosses the water surface. Due to scattering of photons in that region which happens mainly because of the imperfection of optical beam path water at surface. On the other hand since UOWC systems offers very high data rates compared to other available solutions and life time of the key is much shorter.

According to the data protection guidelines shared by National Institute of Standards and Technology (NIST) the keys that is used for encrypting the communication should be used for limited times [23]. For example according to guideline for implementing Asymetric Encryption (AES) 256 Gallois Counter Mode (GCM) suggests

number invocations shouldn't pass 2 power 32. Means the same key cannot be used more than 2 power 32. As a result, the system should find a way to acquire to sustain secure communication.

The deployment and maintenance of these nodes is generally not an easy task and it is quite expensive, because it involves special equipment and trained people to do such tasks. Thats why some of the underwater nodes are designed survive for years depending on application to minimize operational costs. During this very long lifetime of the underwater nodes it is possible that the key inside that node is compromised or it is used so long that it might not be secure anymore. QKD systems can offer secure key sharing between nodes using single photons. Since the quantum secure keys are transferred also wireless it can reduce operational costs and save time for the underwater sensor nodes that needs to be online all the time.

1.3 Thesis Motivation

Despite the increasing deployment of USNs and a growing relevant literature, cyber security aspects have received relatively low attention [24]. Particularly for maritime applications such as the surveillance of critical infrastructure (i.e., harbors, ports, offshore oil platforms, underwater pipelines etc) and border protection, secure communication is the key to ensure the confidentiality, integrity and authentication of the transmitted information. Some countermeasures for cyber attacks have been investigated for USNs [25]. However, all potential solutions offer only computational security based on some mathematical complexity of the encryption. In the quest for quantum advantage, the realization of sufficiently powerful quantum computers is predicted to be possible in the foreseeable future. This would make today's cryptosystems practically useless. USNs are no exception and will be left vulnerable to all types of cyber-attacks bringing a huge threat on maritime security.

The new era of quantum computing brings the necessity of "quantum-secure"

cryptography schemes. Based on the firm laws of physics rather than unproven foundations of mathematical complexity, quantum cryptography promises unconditional security for various marine operations[26]. The Proof-of-Concept (PoC) underwater QKD system presented on this thesis designed to work on relatively short distances under the consideration of several use cases. For example, one specific use case is the pre-mission key exchange. During the initiation phase of a marine mission, various vessels, submarines, and AUVs can update or refresh their keys. For this purpose, they can maintain a sufficiently close distance to the command node for successful QKD operation. Another use case is the updating of secure keys of underwater sensor nodes. These underwater sensors transmit information on a regular basis through acoustic or optical channels, and the keys used in these systems can be updated via the aid of AUVs.

In the last decade or so, significant advances have been made in the area of QKD and successful experimental demonstrations over fiber optic, atmospheric or satellite links have been performed for various transmission ranges and data rates [27, 28]. The current results are however not directly applicable to underwater environments with unique challenges. Underwater optical transmission suffers from severe attenuation as a result of absorption and scattering due to water molecules and other particles in solution and suspension in water [29]. Unlike free space and fiber optic links [30] which typically operate at infrared wavelengths, visible wavelengths are typically preferred to minimize the underwater attenuation [31]. In particular, the blue-green wavelengths outperform the red-yellow-green wavelengths at open ocean [32, 31] while red-yellow-green wavelengths outperform blue-green wavelengths at coastal turbid waters. Especially coastal and turbid waters have more gelbstoff concentration and it mainly absorbs blue-green wavelengths, while being transparent to red wavelengths. On the other hand open ocean absorption is more like a pure water absorption [33] [34].

The initial works on underwater QKD are theoretical in nature [29, 35, 36, 37, 38]. Based on BB84 protocol, the work in [35] investigated both horizontal and vertical links assuming various transmission distances and depths. The study in [36], investigated feasibility of horizontal submarine-to-submarine QKD links. In [37], performance analysis of BB84 protocol over turbulent underwater channels was presented discussing the effect of different water types, weather conditions and various system parameters. Decoy-state BB84 was further analyzed in [38, 29].

Experimental underwater QKD studies are relatively limited, see e.g., [39, 31, 40, 41, 42, 43, 44]. In [39], BB84 protocol with decoy state is implemented using off-line processing and tested over an air-to-water channel. The Alice and Bob (traditional names for the transmitter and receiver units in the QKD literature) are built on optical benches. A waveform generator is used for generating pulses at Alice and a timestamp instrument is used to record measured pulses at Bob. The underwater part of the link is 30 m long, the achieved QBER(Quantum Bit Error Rate) is %2.48 and key rate of the system is 220 bps. [31] presents another experimental study of decoy state underwater QKD where a waveform generator is used for generating pulses at Alice and an oscilloscope is used to record pulses at Bob. The average QBER of signal state is %0.95 and key rate of the system is 711 kbps. [40] uses a spatial light modulator (SLM) to generate different orders of OAM. As wavelengths, 710nm and 943nm are used as idle and signal transmisson signals which are typically not preferred for underwater channels. The work in [41] characterizes underwater channel for quantum communications in the Ottawa River. Their system uses a wavefront error sensor(WFS) and a CCD camera at receiver to analyze effect of turbulence to generated states. At [43] researchers built a 55m long experimental air to water QKD test setup where 6 polarization states are generated and generated states are successfully received with very low distortion more than 95% fidelity. [44] investigates underwater quantum channels in a 30-meter flume tank and use 532nm wavelength.

The QBER is calculated as 0.91 % and key per transmitted photon is measured as 0.84 at 30m after post processing of the recorded information.

The experimental underwater QKD set-ups in the aforementioned works typically use laboratory equipment and off-line processing. The exceptions are [42, 45] which used FPGAs for the development of the underwater QKD experiments. The QKD set-up in [45] implements the decoy state BB84 protocol where FPGA is used for sending pulses and receiving them. All QKD implementation is implemented on an external user PC including the error checking, error correction and privacy amplification. They have reported a final key rate of 245.6 bps with an average QBER of % 1.91 in 2.4m water channel. [42] also implemented BB84 protocol and achieved % 3.5 QBER in 2.37m water channel where FPGA is used just for sensing incoming pulses and sending the timestamp information to computer. The rest of the BB84 implementations are also done on user computers. While their partial implementation builds upon FPGA, the works in [42, 45] still heavily rely on offline processing and computers to retrieve final key.

In this thesis, as a first step towards real-time quantum-secure underwater wireless networks, we develop an underwater QKD PoC built on a hybrid computation system. A real-time photon counting module is implemented on FPGA while the rest of the QKD algorithm works on the (OBC) unit. Since the OBC will handle heavy computing tasks, this design choice is expected to be instrumental in reducing the execution time of the QKD algorithm. To the best of our knowledge, this work is the first fully integrated underwater QKD terminal prototype that processes all QKD operation without any involvement of user. The design relies on one of the most simple and cost-effective FPGA (Intel Cyclone 10 LP) available on market and no external FPGA memory is used on the implementation.

The rest of the the is organized as follows: In Section II, we present the system

architecture. In Section III, we have deep dived in to how realtime QKD is implemented using OBC and FPGA platforms. In Section IV, we have showed the Final PoC and shared experimental results of the system and Section V is the conclusion where we have summarized the current status and shared some of planned potential improvements.

CHAPTER II

SYSTEM ARCHITECTURE

2.1 Overview of System Model

The PoC is built on the BB84 protocol [26]. In BB84 protocol, each binary bit is encoded using a pair of mutually unbiased basis. A typical choice in practice is the use of pre-defined polarization states known as bases. For example, to represent the "qubit zero", either a vertical or a right-diagonal state can be used while a horizontal or a left-diagonal state can be used for "qubit one". During transmission, Alice (traditional name of transmitter in quantum cryptography terminology) randomly swaps between these polarization states. Bob (receiver) measures the photons in one of the two bases chosen at random and records his choices as well as the outcome of detections referred to as "raw key". Alice and Bob then compare publicly the two independent random sets of polarization bases that were used, making use for this purpose of a standard communication channel. This channel is not necessarily optical and can take any form based on the communication application. The bit values of those polarization states measured in the compatible bases yield the "sifted key" and the rest of the raw key is discarded. Any adversary (Eve) can intercept both the quantum and the communication channel. The communication channel however leaks no information to third parties due to intrinsic randomness, i.e., each base has equal probability of resulting in a one or a zero. Furthermore, since quantum measurements are destructive, any attempt by the eavesdropper on the quantum channel will introduce noise into the system revealing her presence.

The conceptual block diagram of system architecture presented in Fig. 1 and overall detailed system architecture is presented in Fig. 2. To generate the required

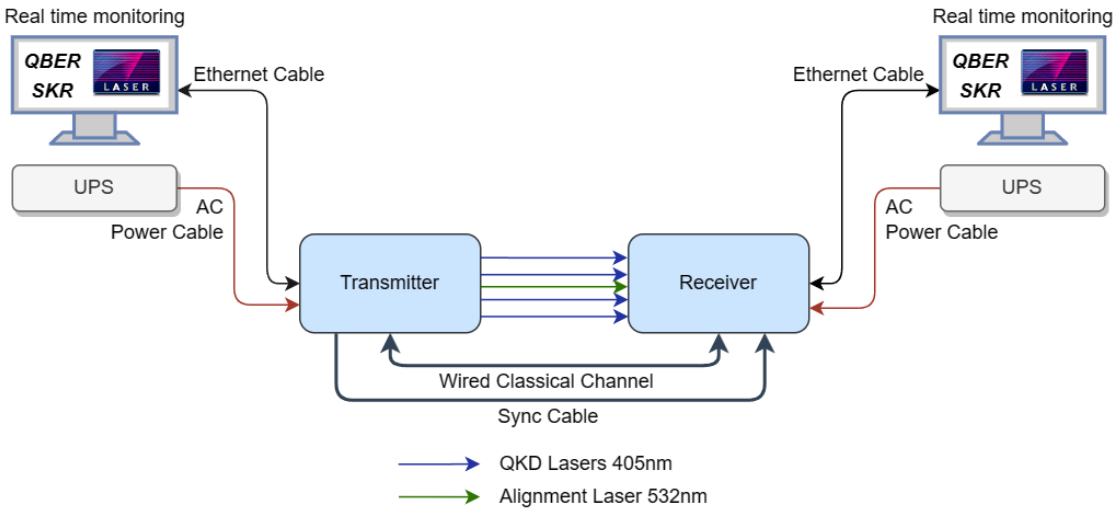

Figure 1: Conceptual representation of QKD sytem

four polarization states at Alice (transmitter), we use single-mode pulse laser sources (denoted by LS1, LS2, LS3, and LS4) operating at 405 nm (blue color). The blue color is selected due to its favorable propagation characteristics in the underwater medium. These four laser sources are driven by an FPGA. Each of the laser outputs is followed by a tunable linear neutral-density (ND) filter, denoted by LNDF1, LNDF2, LNDF3, LNDF4, to attenuate laser pulses. The mirrors (denoted by M1, M2, M3, M4, M5, M6, M7, and M8) are used as pairs with respect to the laser path to perform the so-called "beam walking" and align lasers to the same spot. The mirror pair (M9 and M10) is used to change the beam position for effective utilization of the space. The polarizing beam splitters (PBS1 and PBS2) are used to combine horizontal and vertical polarizations. To obtain +45° and -45° polarizations, we first combine horizontal polarized (0°) LS3 and vertical polarized (90°) LS4, then use a half-wave plate (HWP) denoted by HWP1 at 22.5°. The resulting signal is then fed to a 50/50 non-polarizing beam splitter denoted by BS1. The combined polarized signals are redirected to a constant ND filter denoted by NDF1. The mirrors M14 and M13 are used for the purpose of beam walking and align blue and green (alignment) laser sources at the dichroic mirror denoted by DM1. The spatial filter SPF1 is used to

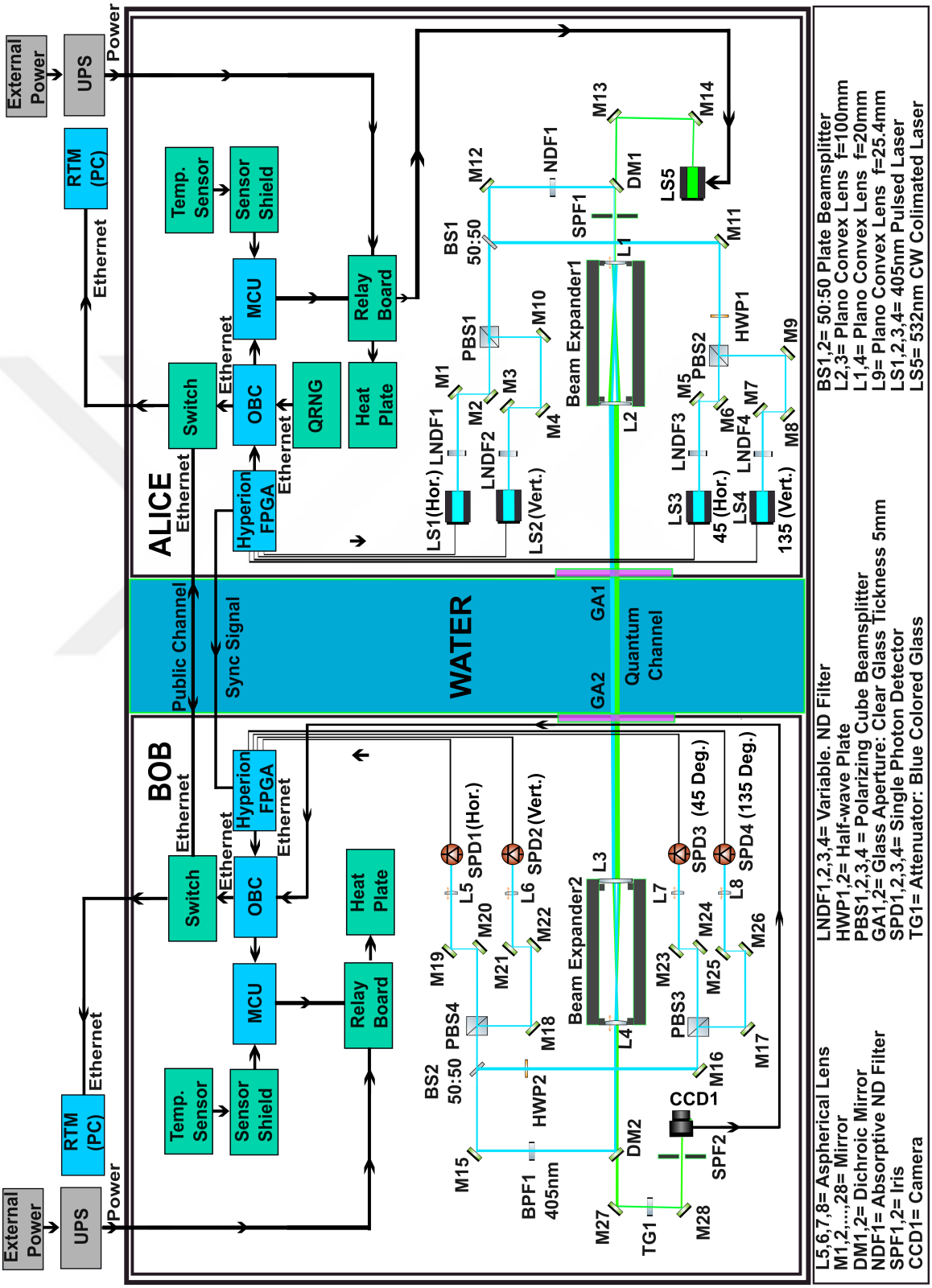

Figure 2: Underwater QKD system architecture.

limit beam size and mitigate back reflections in system. The Beam Expander 1 is used for increasing the beam width to 7.2 mm from 1 mm. The glass apertures (GA1 and GA2) are made with clear glass for minimum loss.

An OEM Quantum Random Number Generator (QRNG) module that provides guaranteed uniform distributed random binary bits at a rate of 4 Mbit/s is used as a random source. It generates the random bits and feeds them to the OBC for the proper selection of the laser modules, i.e., the polarization state. The randomness of data generated keys are verified according to [23]. The OBC provides information on the laser selection to the FPGA. This information is loaded to the block RAM of the FPGA. The FPGA reads this data using a FIFO module and accordingly generates precise short-duration electrical pulses. The timing of laser pulses is achieved by triggering laser diode modules with these FPGA-generated electrical pulses. Moreover, it also communicates with the receiver node over a public channel (Ethernet connection[1] in our case) for sifting. The synchronization of the two FPGA boards is achieved through a coaxial cable. At Bob, the received optical signals from the blue colored (405 nm) lasers and the green colored (532 nm) alignment laser are passed through the Beam Expander 2 to reduce beam width back to 1 mm. Then they are demultiplexed using a dichroic mirror DM2. The green beam is passed through the spatial filter (denoted by SPF2) to limit beam size and blue epoxy glass (denoted by TG1) for slight attenuation. It is then redirected to the CCD1 using mirrors M27 and M28. A 405 nm band pass filter (denoted by BPF1) is used to reject unwanted wavelengths from the incoming photons. Using the mirror M15, the blue beam is redirected to the non-polarising 50/50 beam splitter (denoted by NPBS2). The NBPS2

[1]In practice, this should be replaced by either an acoustic or optical link. In the case of an optical classical channel, data rates exceeding hundreds of Mbps or even Gbps can be achieved. This is 4-5 orders of magnitude faster than the quantum link. If the classical channel is based on acoustics, for the typical underwater QKD distances on the order of 10m - 50m, the acoustic link could provide data rates on the order of 100 kbps which is still well above the quantum link.

randomizes basis selection by blindly forwarding incoming photons to two paths regardless of their polarizations. One path feeds to a polarizing beam splitter PBS3 to obtain polarization states of 0° and 90° while the other path is fed to a HWP2 for 45° rotation. The rotated polarization bases are redirected to PBS3 using the mirror M16 where polarization states of -45° and +45° are extracted afterwards. The mirror pairs (M19, M20, M21, M22, M23, M24, M25, M26) are used for beam walking to align beams at the center of the aspheric lenses denoted by L5, L6, L7, L8. These aspheric lenses focus laser beams to single photon detectors (SPDs) denoted by SPD1, SPD2, SPD3, SPD4 which generate electrical pulses if they detect any photons. The SPDs has less than 60Hz noise and dead time is less than 45ns. The active area of the SPDs is 50um and efficiency at 405nm is 18%.

The output of these detectors are connected to the FPGA for high resolution sampling of the received pulses. This part of the FPGA basically works as a timestamp unit. The FPGA sends the measured pulses to the OBC. Bob's OBC shares the measurement basis information with Alice's OBC through the public channel. Alice compares the received measured basis information with the transmitted basis information. Alice picks 128 samples from the matching bases for the sifted key generation. For error correction, it is possible to use various forward error correction techniques including turbo codes, polar codes, LDPC codes [46]. Due to its simplicity we have used Reed Solomon (RS) coding [47] for error correction. The selected basis measurements and the parity bits are then transferred back to Bob. Using the selected basis measurements, Bob generates the sifted key with the measurements recorded before and uses RS parity bits to reduce the effects of possible errors (e.g., due to noise etc). The parameter estimation phase is not yet implemented.

2.2 Building Blocks of the QKD System

Four laser sources are required to generate the four polarization states in the BB84 protocol. For this purpose, we use four 405 nm (blue colored) single mode lasers from Toptica (see Fig. 3). Each of these lasers has 100 mW output power. Their peak wavelengths and operating currents are provided in Table 1.

Table 1: Laser wavelengths

	Wavelength (nm)	**Operating current (mA)**
Laser 1	404.4	109
Laser 2	406.5	111
Laser 3	406.1	111
Laser 4	405.9	110

Figure 3: Laser modules

As it mentioned earlier the QKD systems requires precise detection of single photons. In our design we have used four ID100 Single Photon Detectors (SPD) from Idquantique which can be seen at Fig 4. This particular SPDs has active area of 50um and efficency of 18 percent at 405nm. The dark count rates of SPDs are just around 51 per second, the exact dark counts of each detector used in system can be seen at Table 2. In other words there be only 51 random erroneous measurements due to imperfection of SPDs. These random false measurements directly effects performance of QKD systems specially if Alice transmits a photon with with same basis and other polarization. If the transmitted photon also makes it to detector, the measurement will be cancelled because it will be counted as coincidence. If original transmitted

photon is failed to reach receiver the dark count will create error in the key. The amount of photons transmitted per second should be order of magnitude higher than dark count number of detectors used in system. This ratio directly effects the minimum achievable QBER in a system. The dead time of SPDs is 45ns means that it can not measure any other photons after it makes one measurement. It can measure photons up to 20MHz.

Figure 4: Single photon detectors

Table 2: Dark counts

	Dark Count Rates (per second)
SPD1	52
SPD2	51
SPD3	53
SPD4	52

The performance of non polarizing beam splitters also plays critical role to perform successful secure QKD operation. The randomization of transmitted photons are generated by the BS. It is important that the P polarization states and S polarization states has close to 50 percent splitting ratio. From Fig. 5 it can be seen that the PBS used in system has around 40 percent P polarization transmission to 63 percent transmission and average transmittance is 50 percent. The same beam splitter used for both transmit and receive parts of our system.

In the proposed QKD system the dichroic mirrors used for combining and splitting the green alignment laser and blue QKD laser. The cut off of dichroic mirror is 427nm.

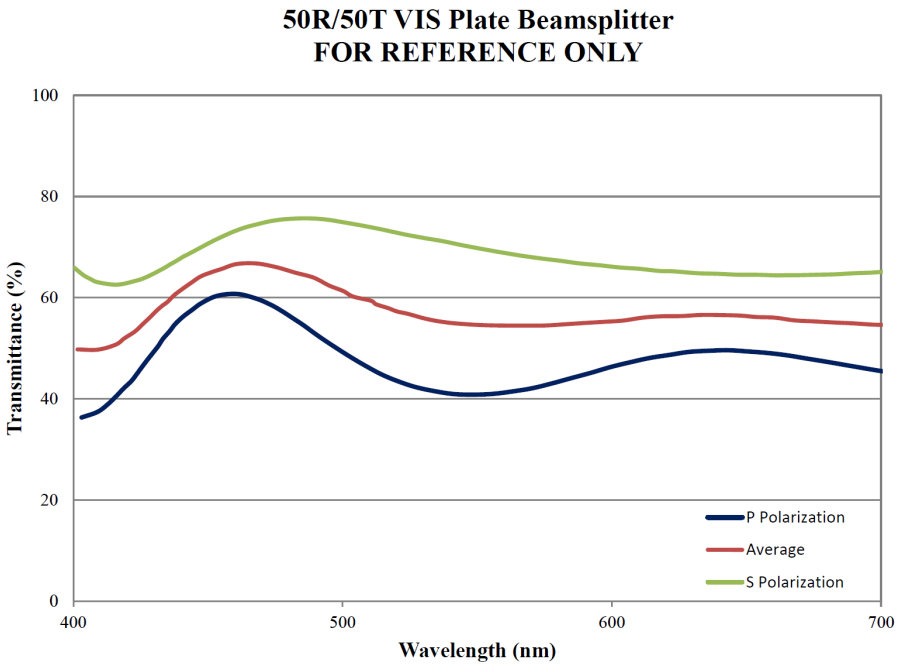

Figure 5: Transmittance graph of beamsplitter

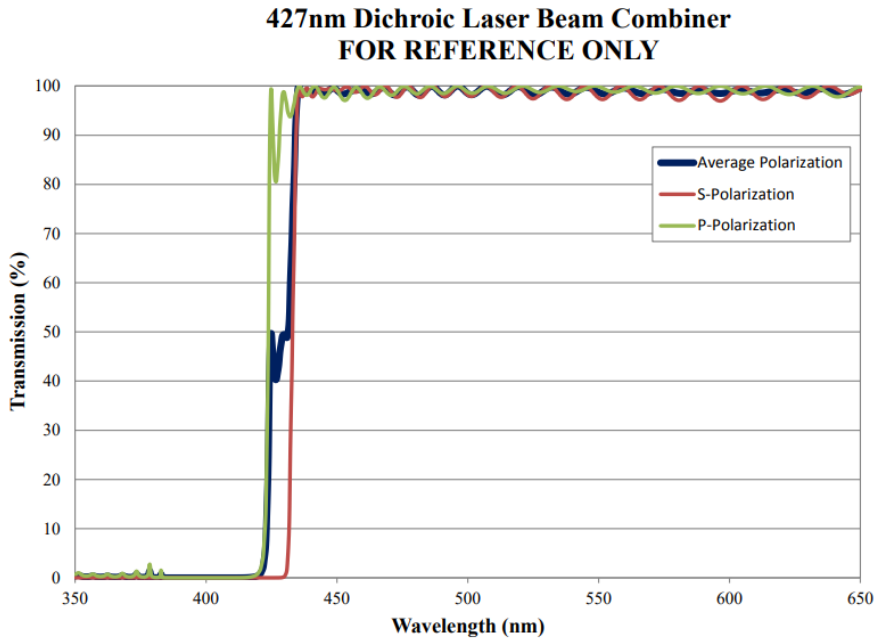

Figure 6: Transmittance graph of beamsplitter

It is sufficiently far from 532nm green alignment and 405nm blue QKD wavelengths. The dichroic mirror has no effect on polarization at 405 and 532nm. The transmission

and reflection graphs can bee seen at Fig. 6 and Fig. 7 respectively.

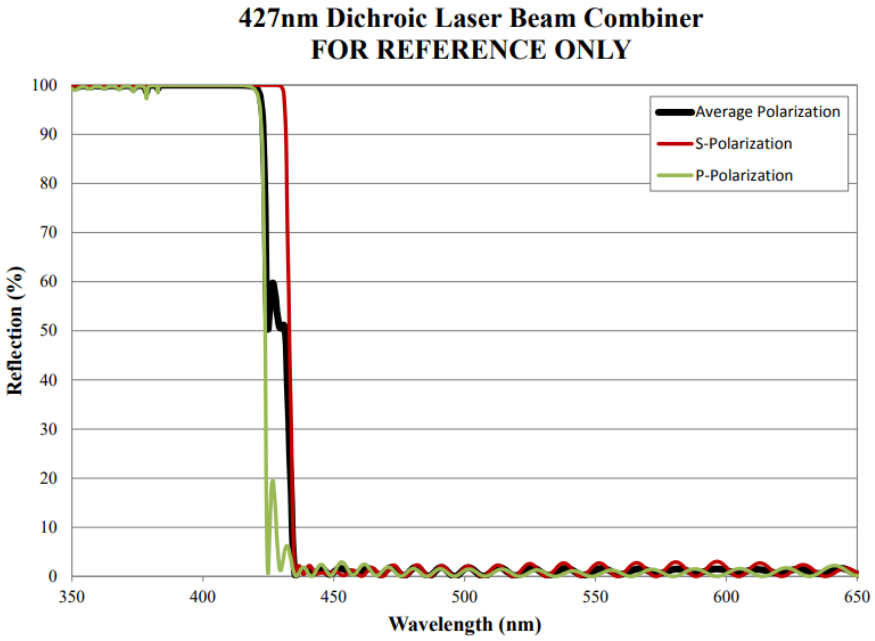

Figure 7: Reflection graph of beamsplitter

In proposed QKD system we have used 28 mirrors to change beam directions to fit complex QKD system in compact chassis and perform fine tuning of internal beams to detectors. The mirrors we choose are specially coated for the 405nm. The wavelength dependent reflection information can be seen at Fig. 8. From the reference measurements of mirrors it can be realized that mirrors are reflective just around 405nm. That makes each mirror to have additional spectral filtering of environmental light. The enviromental light supression is critical for QKD systems which increases chance of coincdadances on detectors thus limits amount of key can be generated from system and if the enviromental light becomes dominant the detectors can get saturated and nothing can be measured at all.

The actual laser diode modules presented in Fig. 3 used in tests which is donated as LS2 in block diagram. The laser modules already has linear polarization output, to rotate polarization to targeted direction we have used a halfwave plate mounted on precision rotation platform.

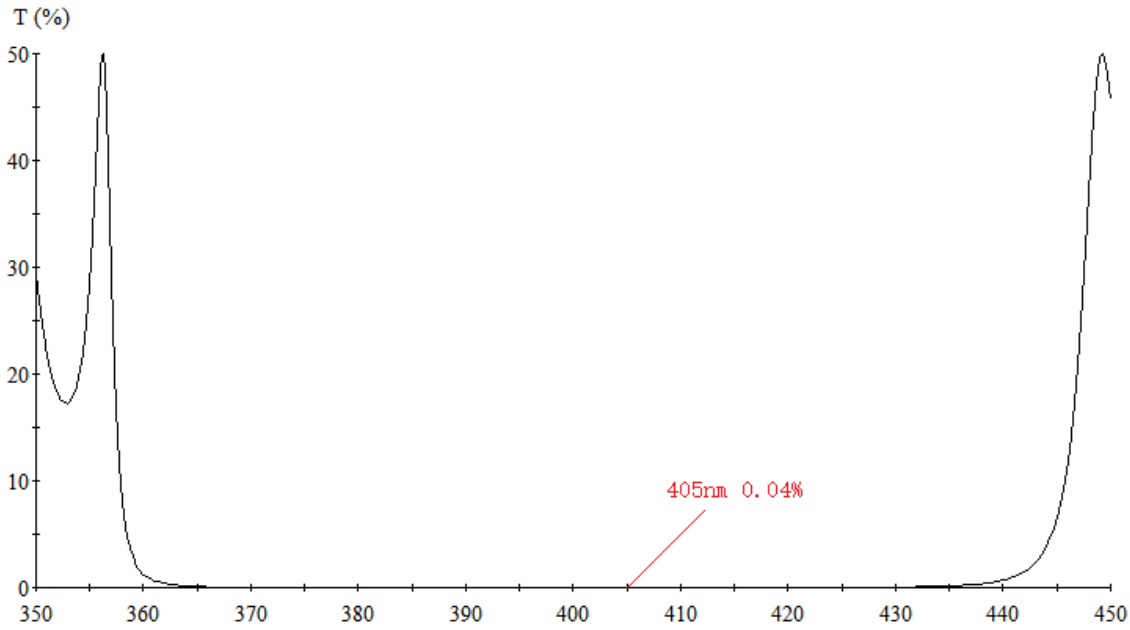

Figure 8: Reflection spectrum of mirror

Figure 9: Linear neutral density filter

Figure 10: Neutral density filter

For transmitter part all of the imperfections on optical and electronics components will be fine tuned by Linear Neutral Density (LND) filters can be seen in Fig. 9. Different from the regular ND filters which can be seen at Fig. 10, LND filters has

attenuation variation horizontally. The LND filters are placed on linear transition stages to precisely adjust amount of light attenuated.

The total system loss analysis of an QKD system is critical to characterise its performance, because of this reason system loss analysis are conducted for each Laser Sources and SPDs. For optical power losses at Alice side Table 3 can be checked. The values on table represents losses for LS1, LS2, LS3, LS4 is after mentioned component in terms of percentage. Before beam expander means all losses before beam expander. "After beam expander" includes all effects including beam expander losses. "With glass apperture" includes effect of glass aperture used in system which is the interface between water and terminal. The LND components are used to equalize the total losses in system to equaliza total output power. As it can be seen LS2 is attenuated much less then other counterparts to achieve equal output power. Each LND fine adjusted to have similiar losses on each polarizations. This attenuation levels directly effects amount of photons in the system, if it is not get equalized one of the laser paths might have more photons in system. As a result it might cause statistical information leak, because one of the bits might have higher chance of transmission compared other bits.

Table 3: Optical attenuation at Alice

Components	**LS1 (%)**	**LS2 (%)**	**LS3 (%)**	**LS4 (%)**
Before Beamexpander	52,51	65,42	56,2	53,28
After Beamexpander	56,03	69,54	60,33	57,53
With Glass Aperture	62,72	73,63	64,91	62,33
LND	23,71	1,2	20,07	15,71
Total Attenuation	71,55	73,94	71,95	68,24

The receiver system performance also depends on how much loss does system experiences due to imperfection at receiver components. The losses at Bob system can be seen in Table. 4. For a successfully polarization decoding the transmitted photons receiver should see minimum attenuation at path that it is originally intend to be transmitted. This means if LS1 is transmits we should see maximum power

Table 4: Optical attenuation at Bob

Components	**LS1 (%)**	**LS2 (%)**	**LS3 (%)**	**LS4 (%)**
Beamexpander to SPD1	61,38	99,49	89,88	77,85
Beamexpander to SPD2	98,45	70,86	77,72	88,19
Beamexpander to SPD3	90,51	67,09	59,01	92,18
Beamexpander to SPD4	74,42	90,78	99,96	73,47
Beamexpander	3,11	5,93	5,25	2,63
Glass	17,01	20,4	21,6	20,7
Total loss for SPD1	68,94	99,61	92,48	82,89
Total loss for SPD2	98,75	78,17	83,45	90,88
Total loss for SPD3	92,36	75,35	69,55	93,96
Total loss for SPD4	79,43	93,09	99,97	79,51

at SPD1, if LS2 is transmits we should see maximum power at SPD2, LS3 to SPD3 and LS4 to SPD4. Means the losses we will see should be minimum in Table. 4 for target tranmit paths and maximum for orthogonal polarizations. If receiver has some leakage to orthogonal polarization means it the chance of transmitted polarization can be recived in same basis, but wrong. This directly increases minimum achivable QBER in system. The losses at beamexpander and Glass are almost equal to each polarization state by slight variations. The leakage from LS1 to SPD2 is 0,39% LS2 to SPD2 1,25%, LS3 to SPD4 6,04% and LS4 to SPD3 is 0,03%. By doing simple calculation using orthogonal leakage information we can calculate minimum achiavable QBER in system. Since we use QRNG as random data source for key generation we can ensure randomisation of data to be correct. Statistically chance of selecting each polarization is same to calculate minimum QBER. The expected value formula can be used to calculate best case average QBER achievable in system. $E(X) = \sum xP(x)$. Maximum achievable QBER in system in best environmental conditions can be calculated as %1.9275.

2.3 Optomechanical Systems

Before the system integration, various optomechanical tests were conducted. During the tests the off the shelf mounts observed were not stable enough to temperature

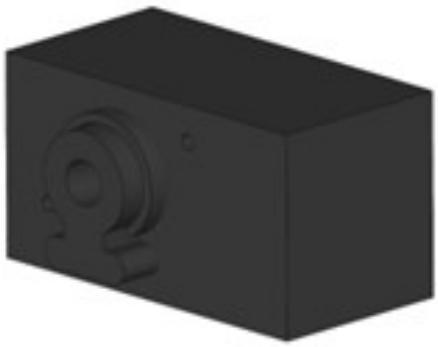

Figure 11: Z stage

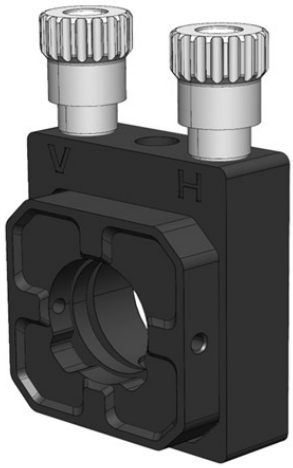

Figure 12: Kinematic mirror mount

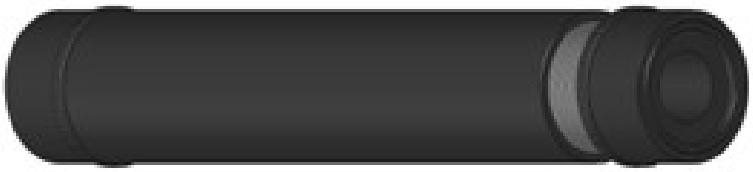

Figure 13: Beam expander

changes, because of this reason custom made temperature stabilised optomechanical parts designed. The Z Stage The Kinematic Mirror Mount and Beam Expander designs can be seen in Fig. 11, Fig. 12, Fig. 13. The effect of temperature changes on the beam expander and kinetic mirrors were tested in the lab environment. For this purpose, the temperature was changed between 0 and 40 degrees. No deformation

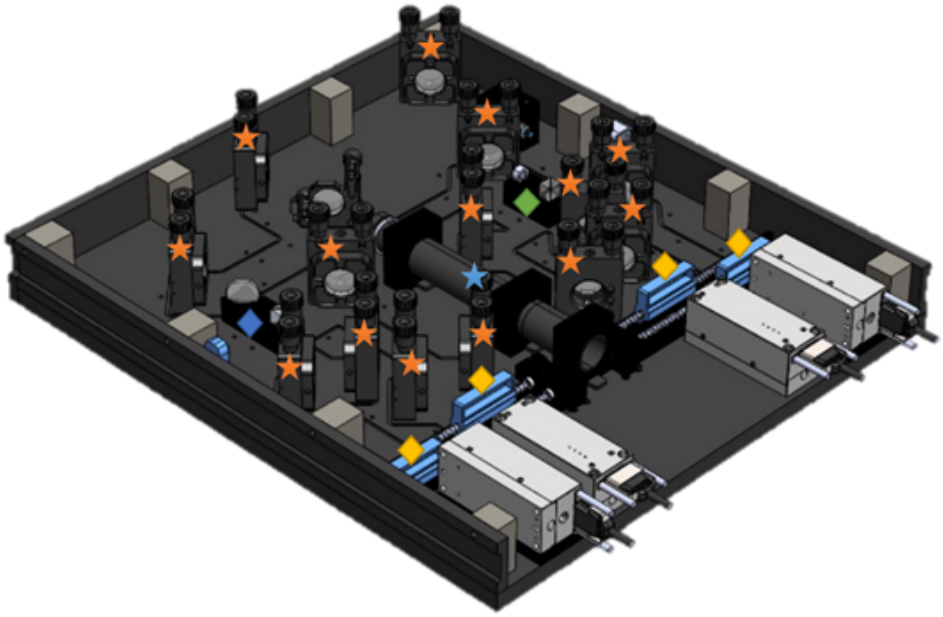

Figure 14: *Alice*

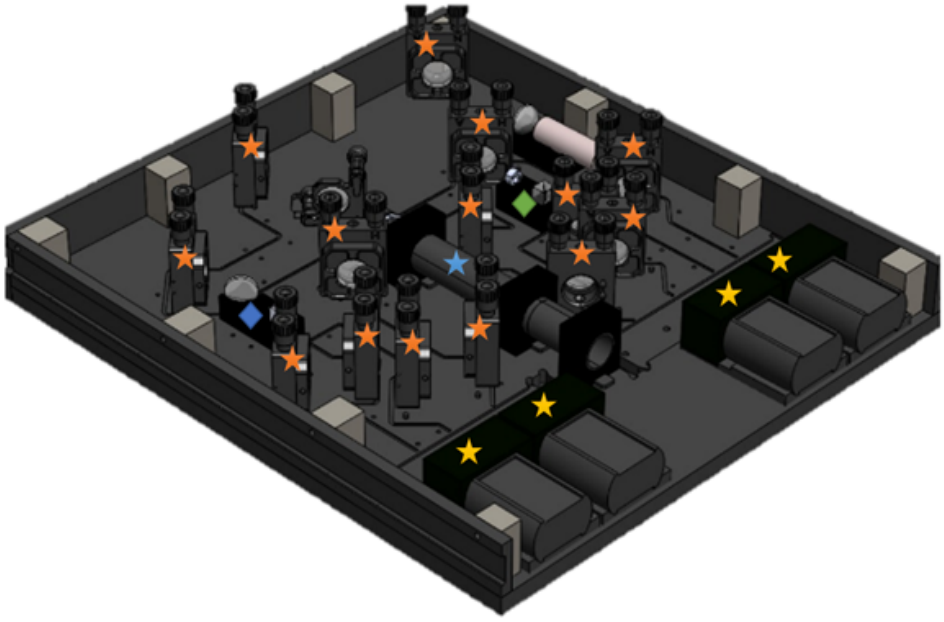

Figure 15: *Bob*

Figure 16: Alice and Bob's optical benches.

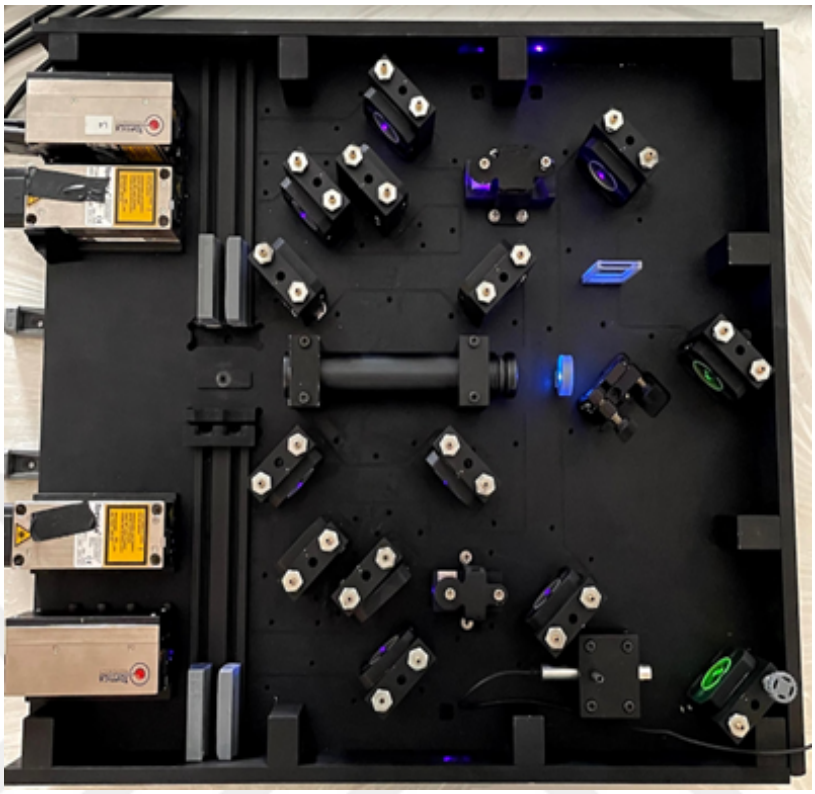

Figure 17: *Alice*

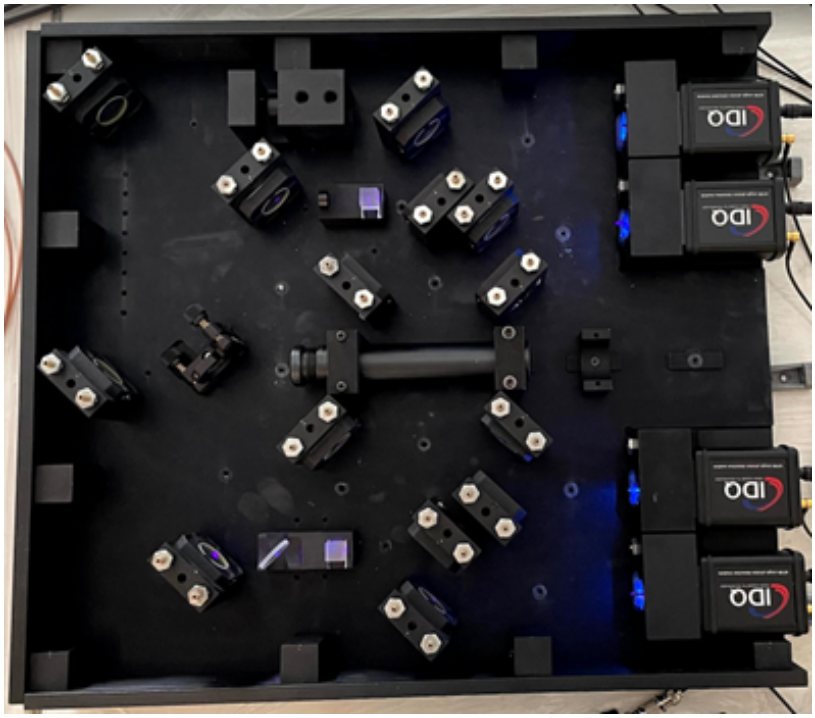

Figure 18: *Bob*

Figure 19: Photo of Alice and Bob's optical benches.

or permanent damage was observed on the mechanical system. The validated sub components were assembled on optical benches following the assembly plan in Fig. 14 and Fig. 15. Different colors are used to denote different components, i.e., orange star - the kinematic mirror mounts, blue star - beam expander, blue diamond - beam splitter, green diamond - HWP, yellow diamond - Linear ND filters, yellow star - SPDs and attached aspheric lenses. Using these benches, laser transmission was successfully tested. Then they were integrated on a rack. The detectors are placed to in reverse direction to main enterance to reduce chance of any enviroment light that enters from optical window to reach SPDs in system.

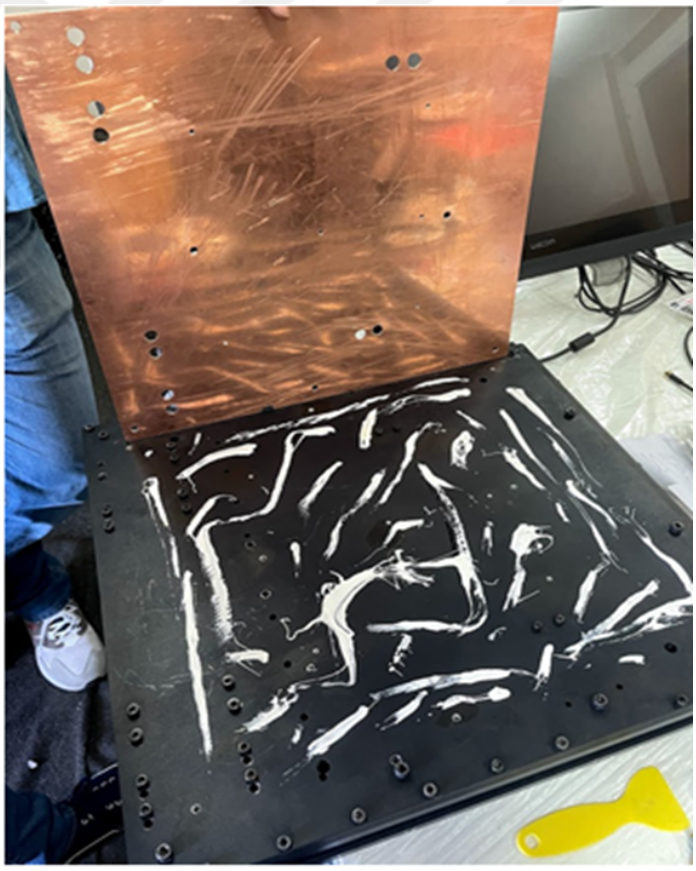

Figure 20: Temperature stabilization plate

The heat plates are assembled to copper sheets to provide homogenous temperature control at each point of the optical benches. The copper plate is then assembled bottom of optical benches with a heat transfer compound applied between them, the

assembly procedure can be seen at Fig. 20. The assembled final versions of Alice and Bob optical benches are provided in Fig. 17, Fig. 18. One of the design challenges is alignment and temperature stabilization of such systems, because underwater temperature levels are much lower than the actual calibrated temperature and the thermal expansion might create misalignment inside of optical benches. To solve this issue, we have implemented a temperature stabilization system for optical benches. Under the consideration of maximum sea temperature is around 30,2 we have stabilised internal temperature of the system to 35 degrees.

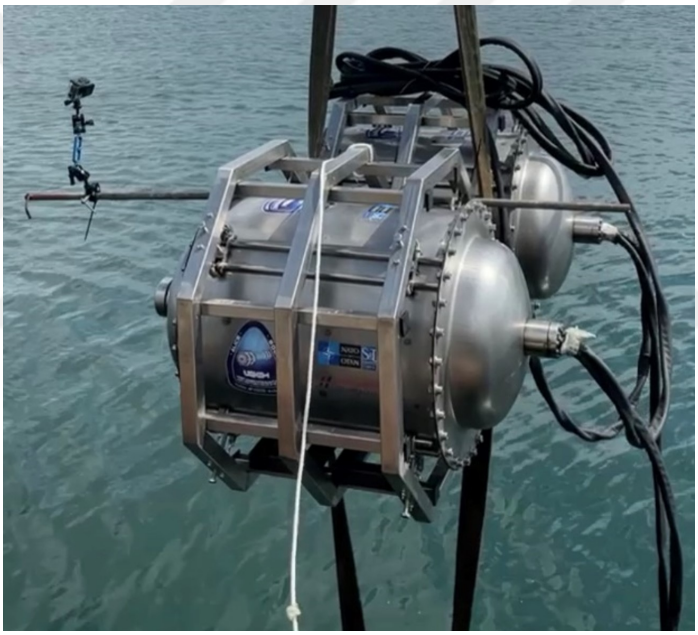

Figure 21: Chassis pressure tst

The outer chassis made out of stainless steel in round shape to withstand underwater pressure. Pressure tests are conducted at opensea by connecting Alice and Bob chassis together and attaching them 470kg of additional weight to keep them at 10 meter depth. The test conducted for 3 hours. The cameras attached inside of the chassis to detect any potential leakage. A picture from that test procedure can be seen at Fig. 21. The Alice and Bob optical benches then mounted inside of the verified external chassis. The rails that holds optical benches welded internal

part of chassis precisely using custom made laser welding reference mechanics. The precision of welding process is critical to minimize angular difference between optical glass aperture installed at chassis and the beamexpanders that transmits and receives photons through that window. That can potentially create distortion on polarization angles and might create unbalance at transmit and received polarisation states. After successful completion of pressure test and completing precise welding optical benches and electronics assembled in to chassis using custom made rail system.

CHAPTER III

REAL-TIME SOFTWARE DEVELOPMENT

3.1 OBC Design

The OBC[1] is a fan less industrial computer durable to harsh environments such as dust, humidity and high/low temperatures. In our implementation, we used the OBC provided in Fig.22. This is equipped with a high performance CPU Intel i7 8700. It further features 4 x RS232 interfaces, 4 x USB, and 2 x Gigabit Ethernet. One gigabit Ethernet is used for public channel communications and the other one is used for communication with the FPGA. Different from Bob Alice also uses RS232 interfaces to control laser modules and one of the USB channel of Alice OBC is used for retrieving QRNG data from QRNG module. The Electronic system diagrams are shown at Fig. 23 for Alice and Fig. 24 for Bob. The power is provided to system through UPS (Uninterruptible Power Supply). This inherently provided system voltage regulation and short circuit protection in case any leakage occurs during trials. There are also Shock Protection Fuses installed inside of the Chassis to isolate system from power quickly as possible.

The MCU controls heat plates through Relays and it is controlled by OBC for temperature target. The system is tuned for 1 degree temperature difference tolerance to keep system in safe operation range during tests. Temperature, humidity and light intensity sensors periodically read by MCU and provided to OBC upon OBCs request.

[1]The SoC(System on Chip) FPGAs are powerful alternatives when flexibility of programming on ARM CPU and real-time processing capability of FPGA is needed. Different from the [48], we have aimed to build a system that completely isolates users from all QKD operations. It can be readily checked from that it still requires a PC to make offline processing of the retrieved data. This indicates that adding SoC FPGA did not avoid using powerful external processors in the overall system architecture. In addition, our system is quite flexible; the OBC (Intel i7 CPU) and FPGA parts can be easily replaceable.

Figure 22: Onboard computer

The MCU also controls SPD and FPGA power through relays. The MCU is powered on automatically when power is provided to system. Once MCU is powered on safely it powers on OBC and waits further commands to arrive from OBC.

As soon as OBC is powered on it checks for MCU connection. Then it control which relays will be opened in the current operation. Afterwards it initiates MCU to start temperature stabilization of system to be prepare system to be ready for QKD operations. OBC regularly checks MCU to validate temperature stabilization of optical bench. MCU takes average of temperature sensors placed in the system and uses its average to estimate general temperature. Due to heat expansion the thermal gradient between sensors limited to 1 degree Celsius difference, if one of the temperature sensor is more than 1 degree average system considers this as stabilization is not achieved. MCU software flowchart can be seen in Fig. 25.

The Alice OBC acts as master controller of QKD operation. All requests are originated from Alice. In Ethernet messages transferred through network first byte used as originator identification 100 used for Alice 101 used for Bob. The Second field is used for identifying packet type rest is attributes related to that particular packet. The simplified function flow of QKD is shown at Fig. 26. In that figure the internal states of Alice and Bob and transmitted packets through public channel are provided. The color code of the shared diagram is as follows blue is OBC internal processing states, purple is specific for commanding laser modules, red is for QRNG

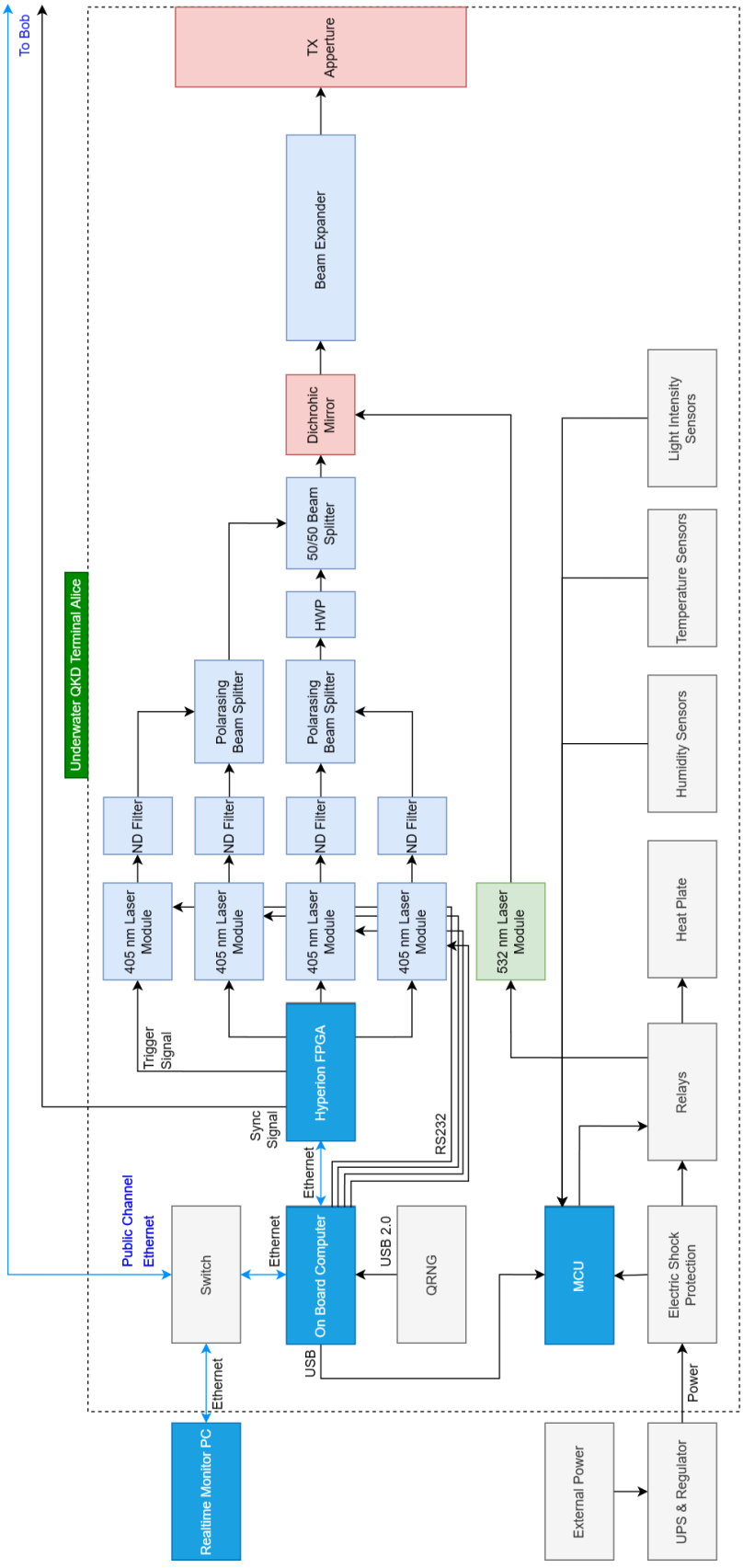

Figure 23: Alice electronic systems

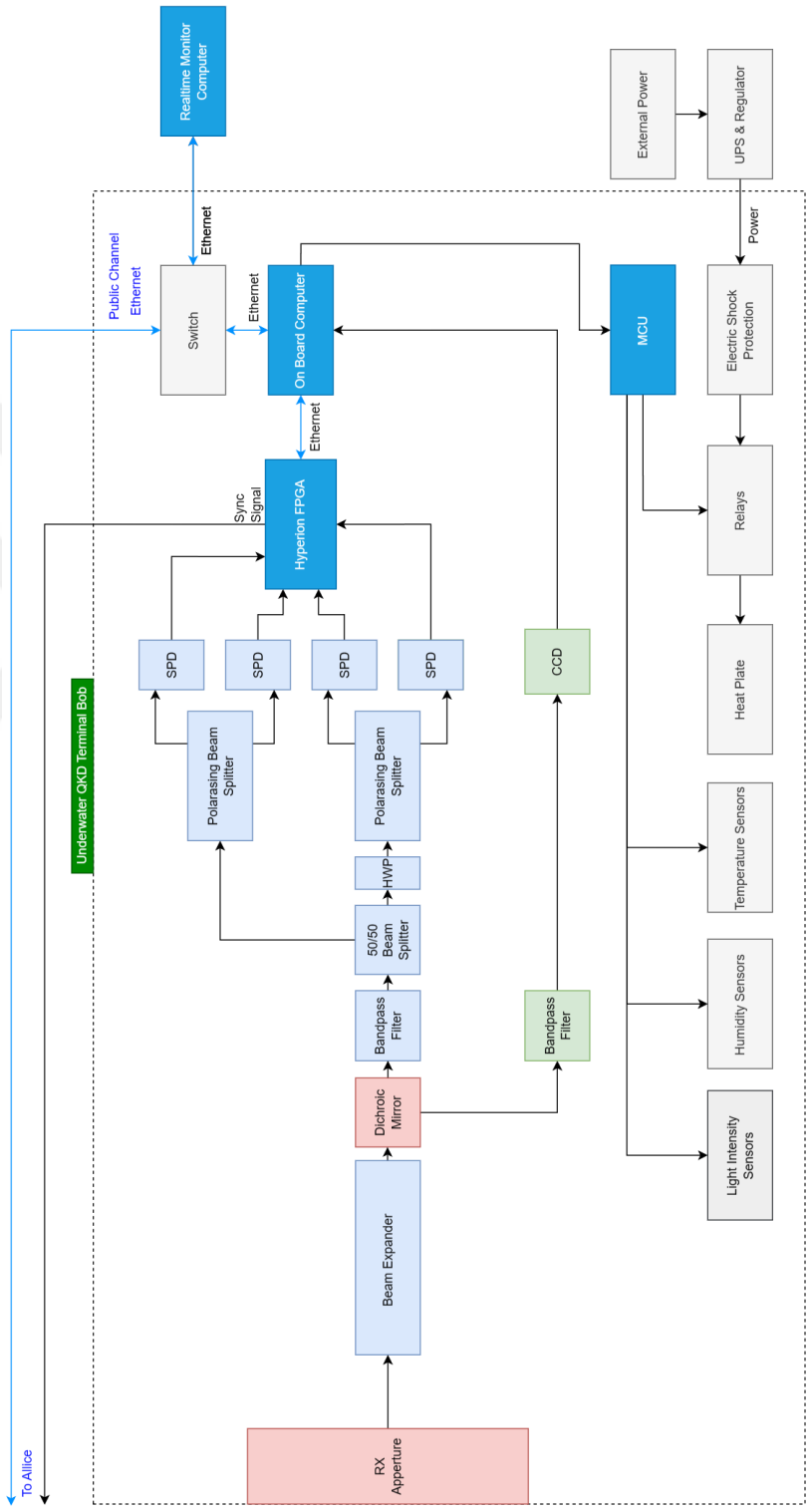

Figure 24: Bob electronic systems

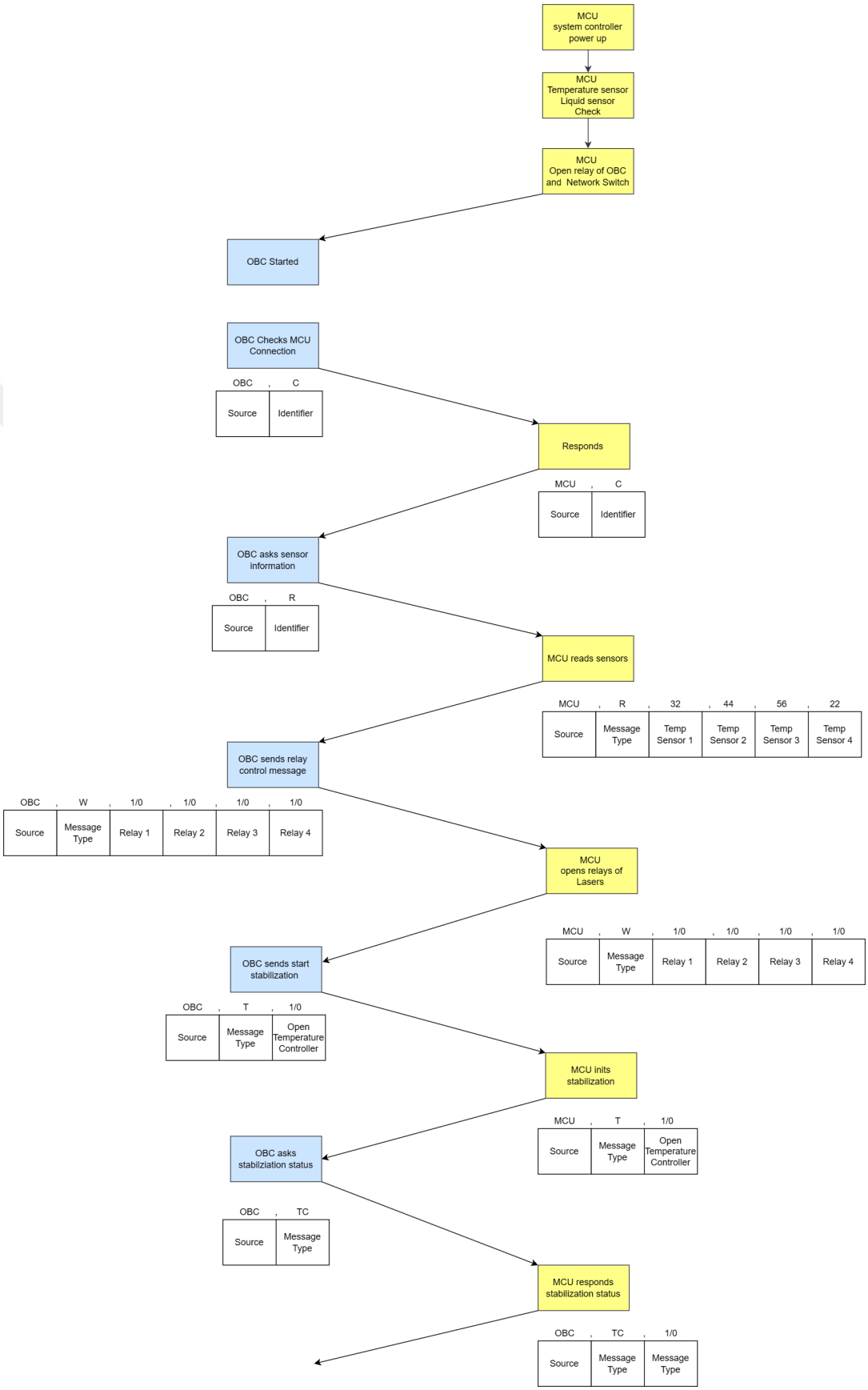

Figure 25: MCU software flow

commands greens are FPGA based communications.

The QKD operation is initialized from Alice. Once QKD Initialized at Alice side it quickly checks fundamental components of system are connected and operational, such as QRNG module and FPGA. Then it informs Bob by simple QKD mode, after Bob completed its own internal checks Bob replies with done or fail message. The main presquite of entering QKD mode is being sure that temperature stabilization at MCU side is completed for both Alice and Bob. At same time Alice sends a message to MCU to power up Laser Modules using relays. Once Laser Modules are turned on Alice OBC recognizes their active connection through RS232 channel. It sets all lasers to pulse mode and tune each laser to a power levels that is previously identified during system loss measurements. Once Alice completed setting up it laser modules it generates a QRNG sequence and parses generated key sequence to 2 bit selections. Each 2 bit selection is used for picking up a laser in system. The generated samples are then loaded to FPGA memory through direct ethernet connection to FPGA. The transmission is started and completed automatically at FPGA side. There are no OBC intervention after start command transferred to FPGA. The accurate pulse timing achieved by handling all these time critical operations at FPGA side. The bob part starts recording of incoming pulses by waiting for trigger signal through sync cable.

Once QKD is completed Alice asks Bob whether transmitted QKD sequence received by bob or not. The bob responds with successful or unsuccessful transmission information. If it is correct Alice asks for basis measurement information from Bob. Bobs OBC requests from the its FPGA to transfer all pulses recorded during measurements. Bob creates packet stream with attributes of packet length with 4 bytes and basis information and time information of every pulse recorded during measurements. During this stream phase Alice records all packets until it receives Measurements Transmit Done packet from Bob. Alice compares received data with

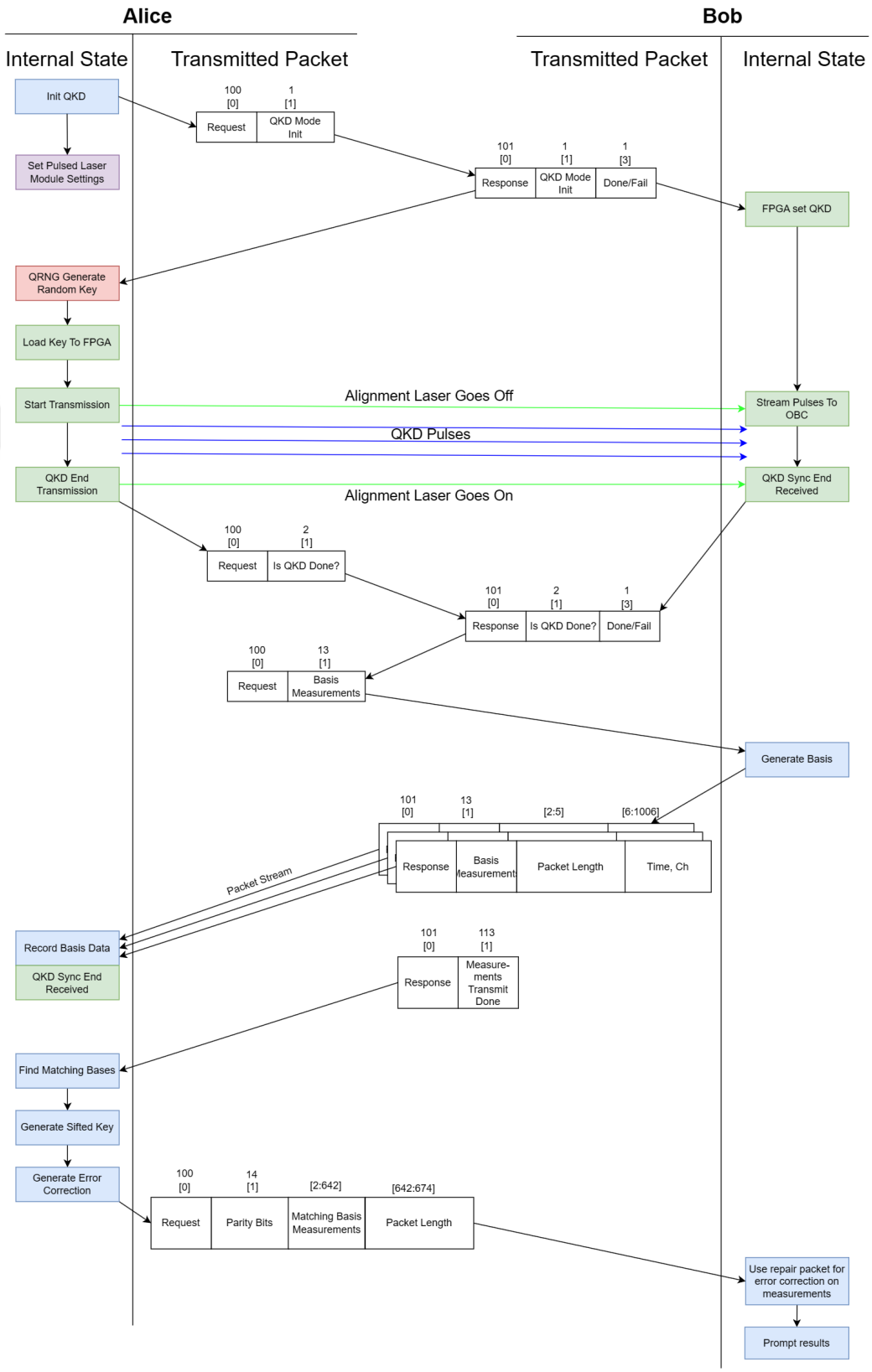

Figure 26: QKD function flow

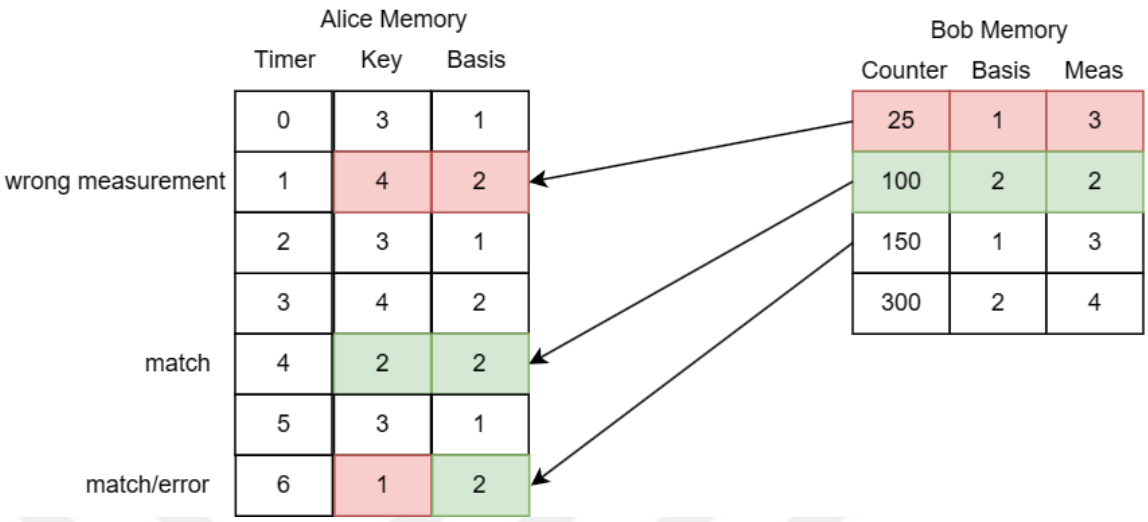

Figure 27: Basis comparison

pulses with the pulses it loaded to FPGA.

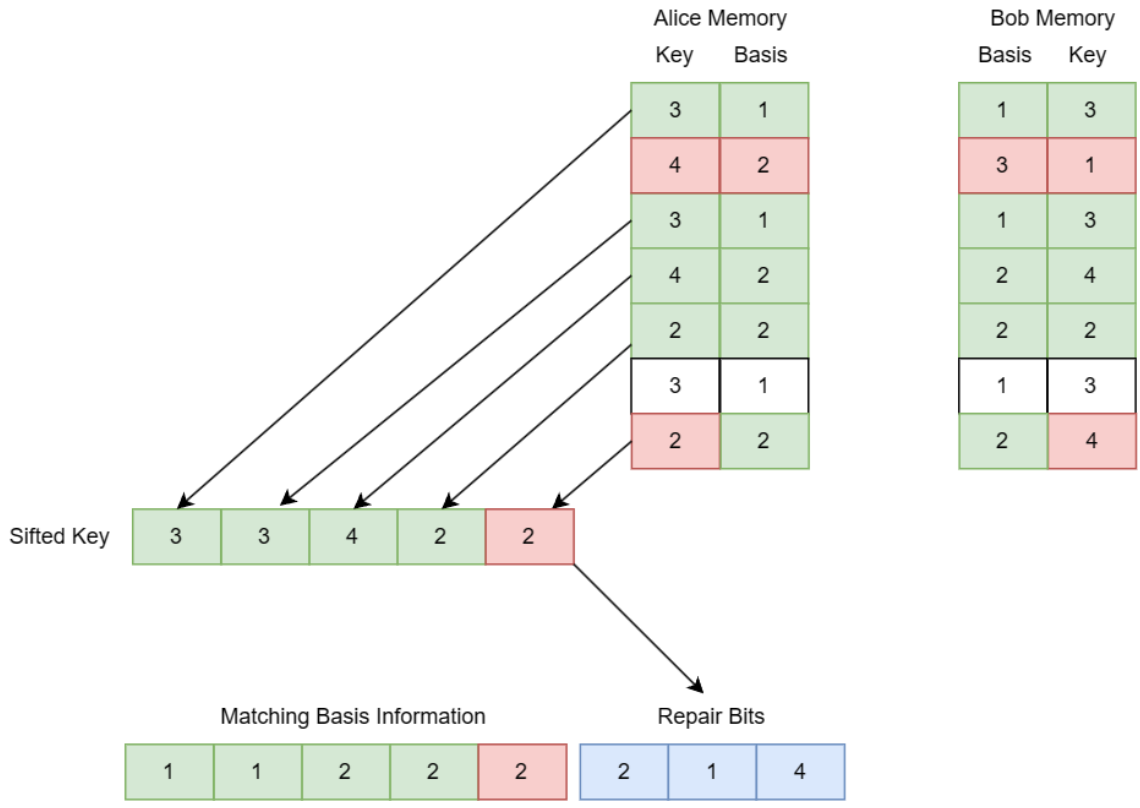

Figure 28: Sifted key generation

The basis comparison process is shown in Fig. 27. The timer column below Alice side is the Alice clock that triggers pulses at 10MHz clock rate. The Bob memory

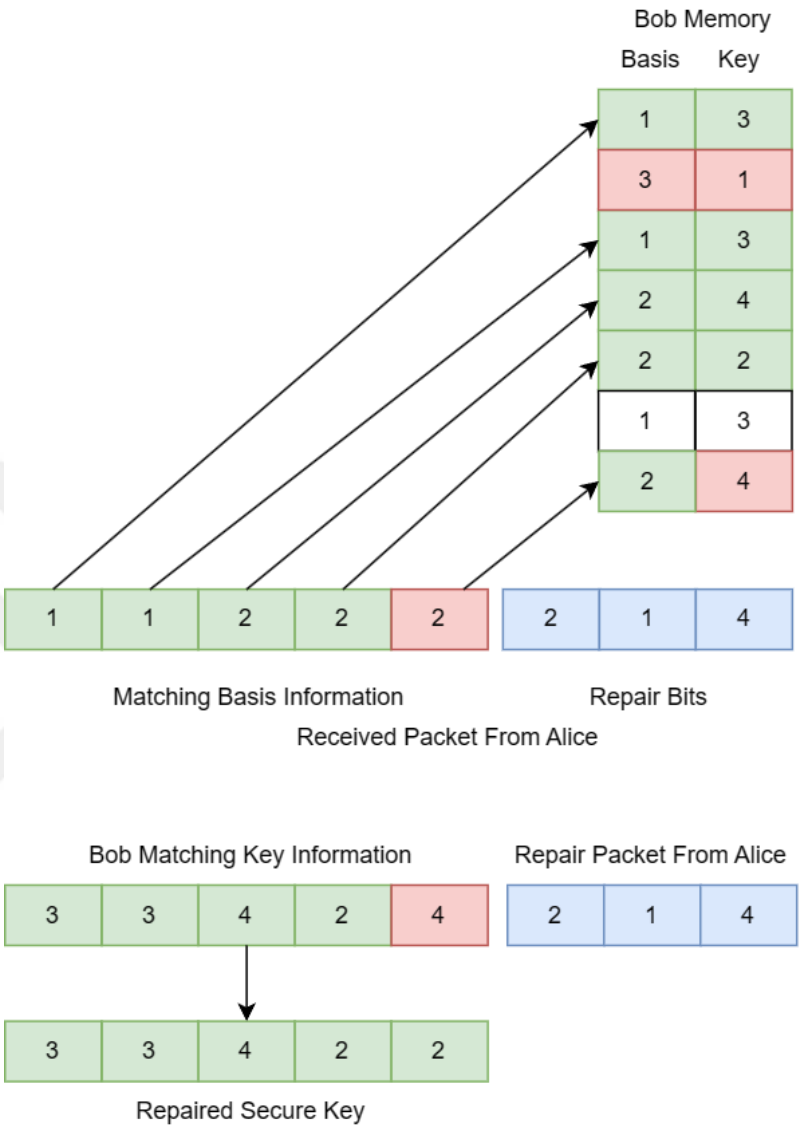

Figure 29: Bob secure key generation

runs at 250MHz. Thus, 25 times more clock ticks expected between correct measurements at Bob. Key is secret key generated using QRNG data and Basis information is the basis information generated internally for comparing Bobs basis information. 4 different conditions highlighted on the Figure. These are lost photons case; where Alice sent pulses and Bob measured nothing at that time. Basically these photons are lost during transmission, potentially absorbed by water particles or scattered to

a another direction. The other case is highlighted as red key red basis. This one indicates Bob measured a photon in wrong basis, since Alice didn't do any measurements at that time Alice discards that unmatching basis. This can be caused by dark counts of detectors or external light measured by detectors. Third case is Match Case. It is indicated with Green Colored on both Key and Basis bars. The photon that is transmitted is measured by Bob correctly. Other interesting case is Matching Base but wrong keys. This is generally happens because of highly turbulent water which might disturb polarization of transmitted photon or due to imperfections in the system. This imperfections are generally coming from polarization beam splitters and optical windows used in system. This kind of errors directly increases quantum bit error rate in the system, because the matching basis is only information that is shared publicly and Alice can not distinguish which key is erroneous measurement and which is correct. The initially generated key which has some errors is named as Sifted Key. This key generation phase can be seen in Fig. 28. Using the original key information Alice applies Reed Solomon algorithm to generate a repair packet. The generated repair packet is tuned to correct only 10% of errors in data. The 10% is chosen to stay below QBER rate whether channel is secure or not. If the errors in system exceeds 10% key can not be recovered. The matching basis information and generated repair packet then sent to Bob for secure key generation Fig. 29. Bob checks for selected matching basis information from Alice then it generates measurement data to generate a sifted key. Then it applies the repair packet on the measurements to find out whether there are any errors exists on the key or not. The resulting key can be called secure key after this process.

3.2 FPGA Design

The underwater QKD system is designed to operate in two main modes, namely "Alignment Mode" and "QKD Mode". The alignment mode is useful to assist the

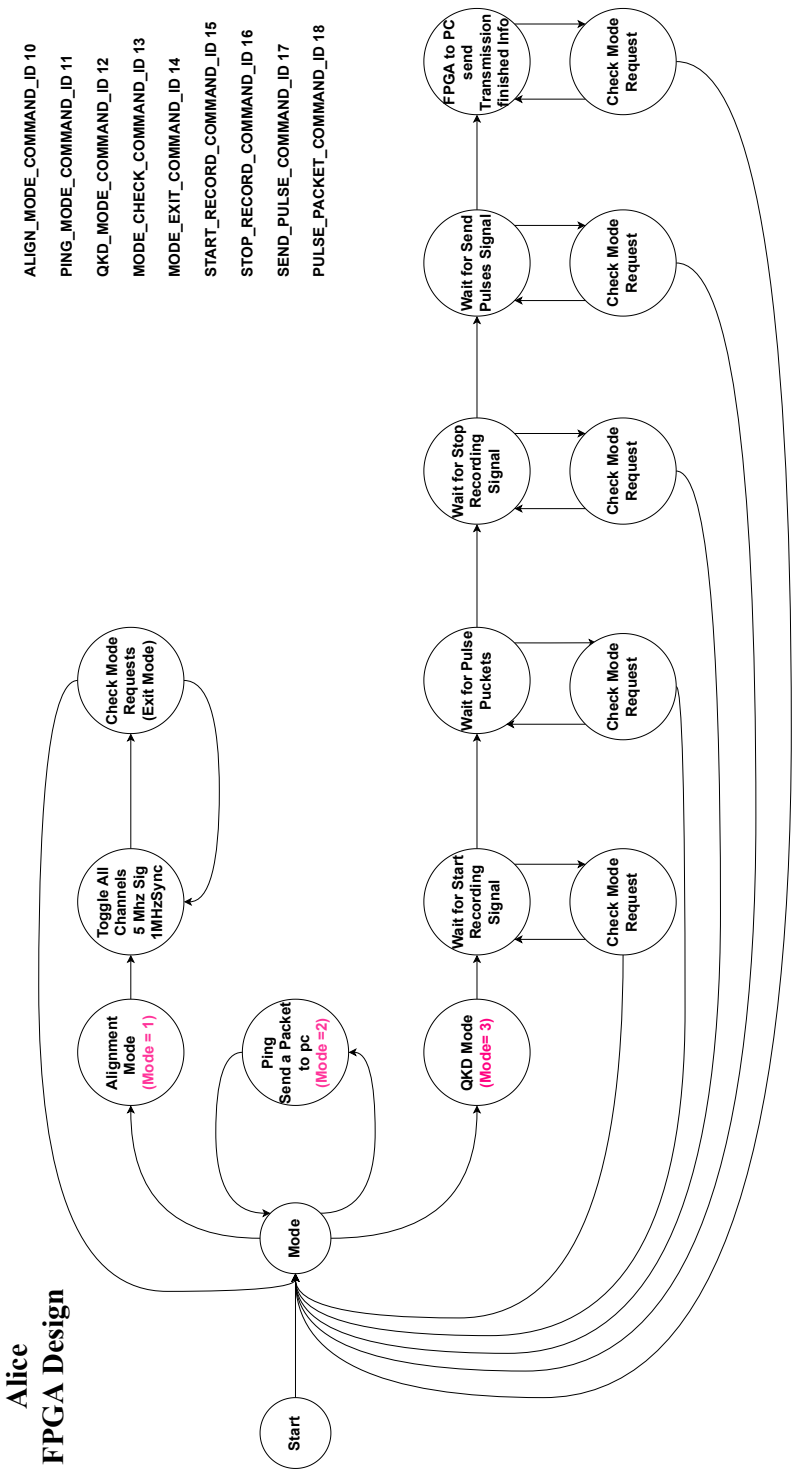

Figure 30: Alice FPGA architecture.

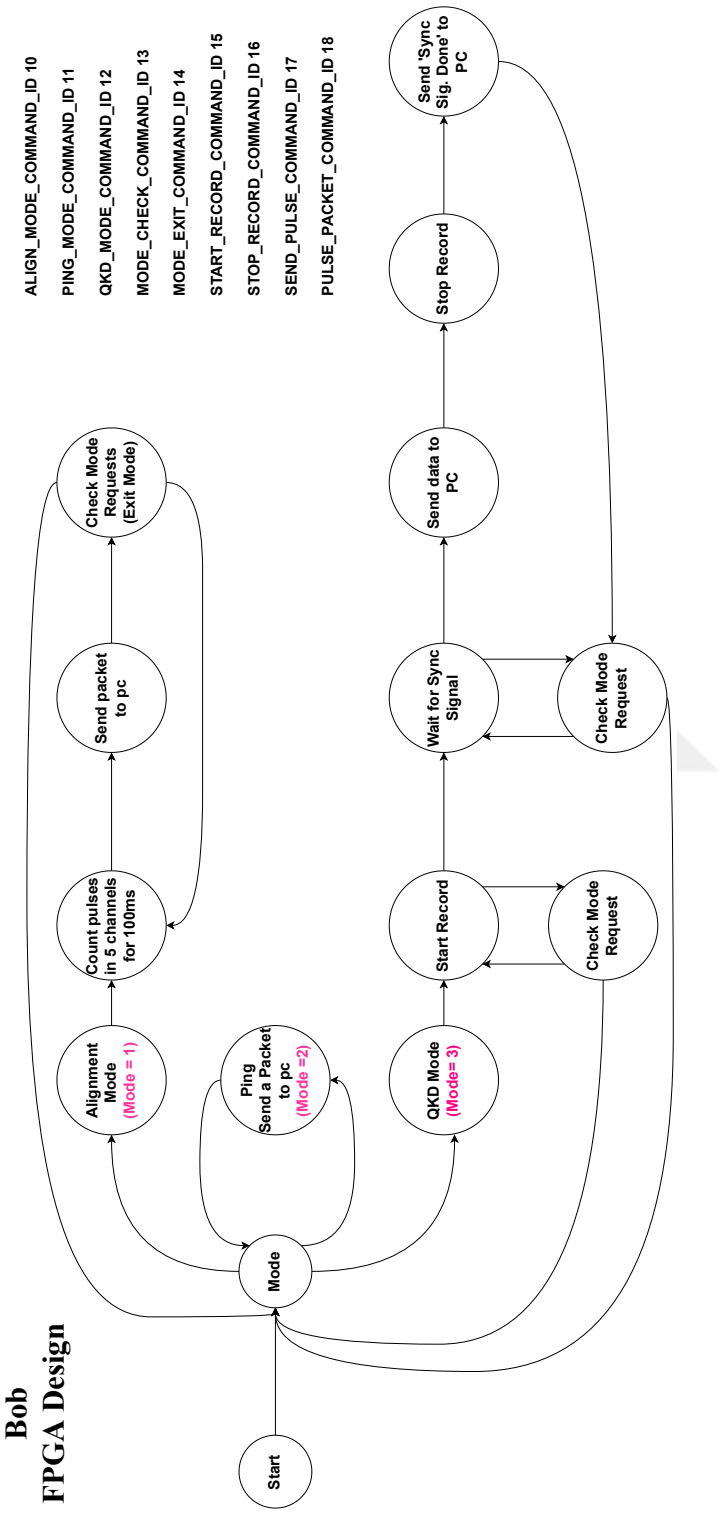

Figure 31: Bob FPGA architecture.

system operator during the manual alignment stage. In this mode, Alice sends continuous pulses to all four lasers and Bob records the amount of photons received in the last 100 ms. The operator can make small adjustments in manual alignment by referring to the received photon counts on each detector. In the QKD mode, the system runs a full BB84 cycle and generates 128-bit keys in each successful QKD iteration.

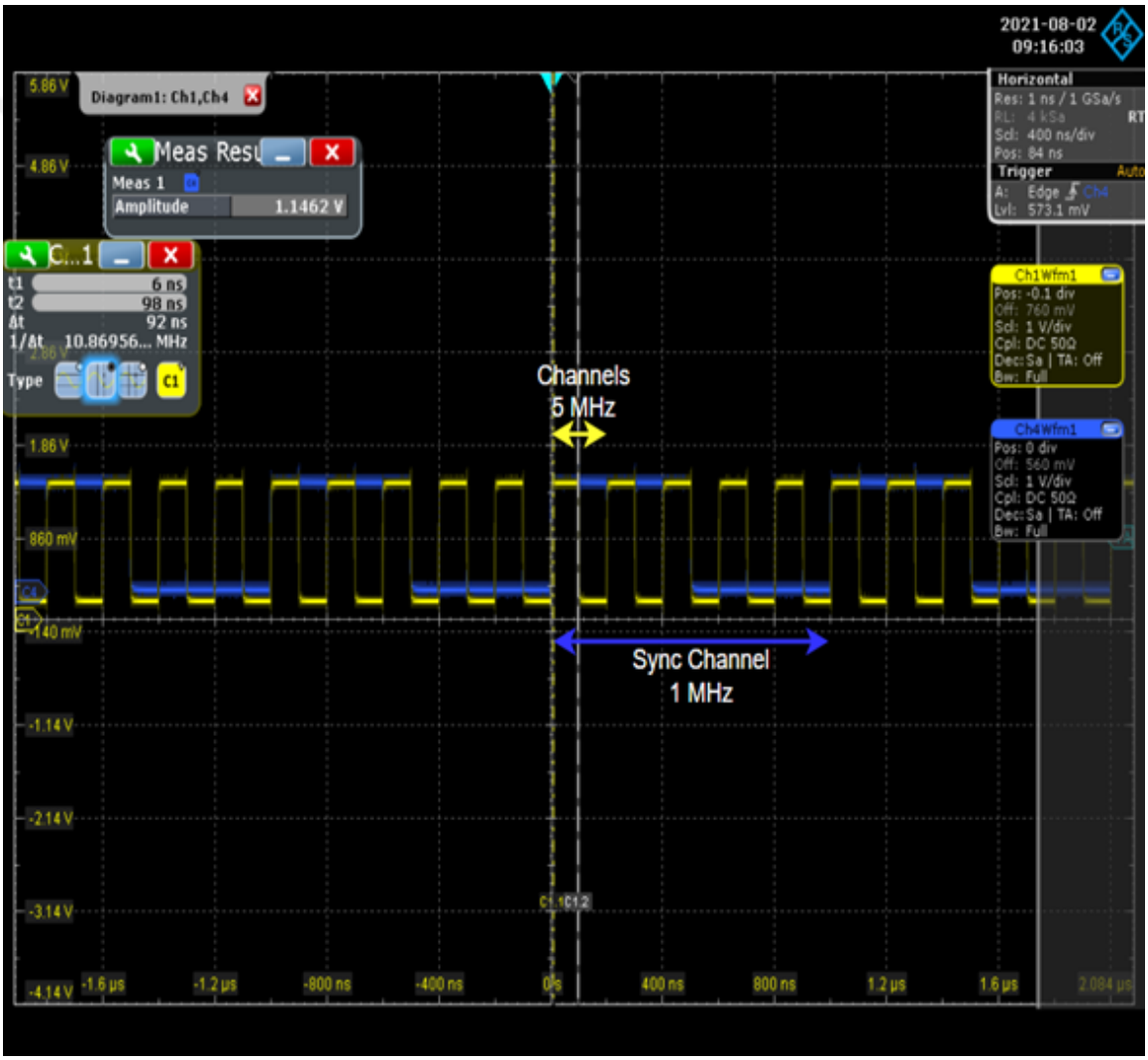

Figure 32: Output signal of the FPGA when alignment mode is on.

Although the hardware designs of Bob and Alice's units are identical, their digital design differs. Their flow charts are respectively provided in Fig. 30 and Fig. 31. As can be seen from Fig. 30, once Alice receives the alignment mode request, it toggles

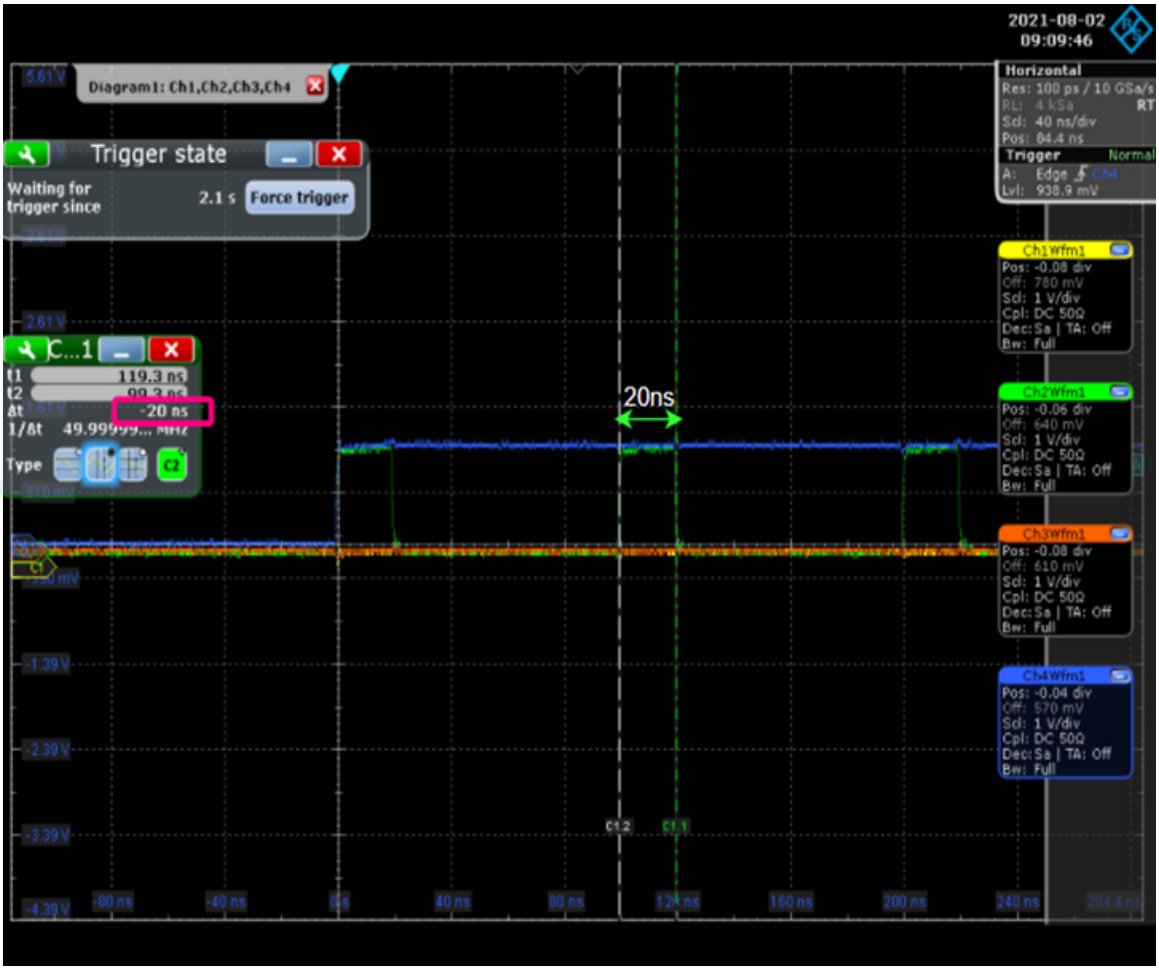

Figure 33: Output signal of the FPGA when QKD mode is on.

all lasers at 5 MHz and 1 MHz sync channel. Synchronization is made by a cable in our implementation; a similar signal is provided through that channel to check possible cabling issues. The photon generation in QKD is a time-sensitive process and the transmitter should generate photons with a very accurate timing. To prevent any delays while transferring the QRNG laser selection information from OBC to FPGA, the OBC first loads the desired laser selection sequence to the FPGA. When the QKD mode request arrives at the FPGA, it switches to a state where it records the incoming pulse sequence. After the process of loading the pulses to the FPGA is completed, the OBC transfers the "stop record" pulse and the FPGA waits for the "send pulses" packet from the OBC as a final trigger to send all the recorded pulses.

When the FPGA receives the "send pulses" command, it starts generating 20ns pulses with the repetition rate of 10MHz to lasers according to the information stored in the block RAMs of the FPGA, and at the same time it sends a logic (high) signal to the synchronization cable. After completing the transmission, it returns back to the beginning of the QKD mode state to wait for the next QKD cycle. The measured pulses generated by FPGA can be seen in Fig. 33. The logic high signal transmitted through synchronization cable is blue colored. Green pulses are the pulses for laser trigger signals.

As can be seen from Fig. 31, during the alignment mode, the FPGA switches to state to counting the pulses from all four detectors and the sync channel. It then sends the recorded pulse counts to the OBC in every 100 ms. In addition, to accomplish timing at Bob's side, it loads the incoming information to the block RAM of the FPGA and sends the measured pulse information to the OBC. When QKD mode is activated, Bob waits for the sync signal which is sent by Alice at the same time when Alice sends pulses to the lasers.

The initial tests of the developed underwater QKD system were conducted by directly connecting Alice and Bob's FPGA ports. Fig. 32 shows the output ports of Alice during the alignment mode. The blue channel is the sync channel and it is toggled at 1 MHz. The yellow channel is the signal that goes to all four lasers, which toggles at 5 MHz. The Sync Channel clock and Signal Channels clocks are generated using the same clock source and Signal Channel and Sync Channels are perfectly synchronized. To test Bob's alignment mode, the Wireshark network sniffing tool was used to capture the generated packets with the count rates of all channels in the last 100 ms. The ping modes of Alice and Bob are similar. The unit sends a predefined packet to the OBC until the exit packet is transferred.

3.2.1 Details of FPGA Implementation

The custom designed credit card sized FPGA board can be seen at Fig. 34. Same FPGA HW used for both Alice and Bob. There is MXM connector placed on FPGA board where the transmit and receive signals received via daughter board. The design done in extendable form to ease implementation of all detectors and lasers on a extension board in future by keeping the most complicated FPGA HW design same. In our study, we developed a transmitter structure that can generate signals for four channels at the desired time and a receiver structure that records the arrival times of signals from four separate channels. In order to transfer the relevant signals to a computer, various auxiliary modules were developed and a receiver and transmitter system has been created. The internal structure of the transmitter system is given in Fig. 35.

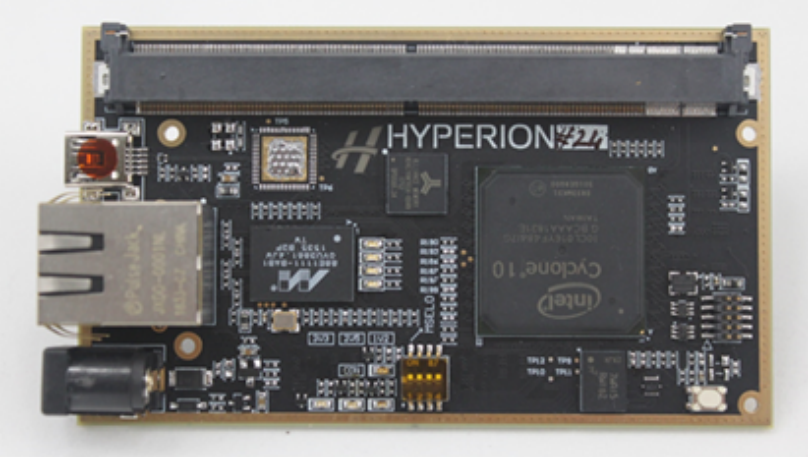

Figure 34: Custom designed FPGA board

The transmitter includes Ethernet IP, MDIO (Management Data Input/Output) Manager and Packet Creator modules. FPGA Ethernet Media Access Control (MAC) IP refers to a pre-designed and tested digital logic circuit that implements the MAC layer of the Ethernet protocol in an FPGA device. This Ethernet MAC IP is responsible for controlling the flow of data on an Ethernet network, including handling the transmission and reception of Ethernet frames and performing error checking.

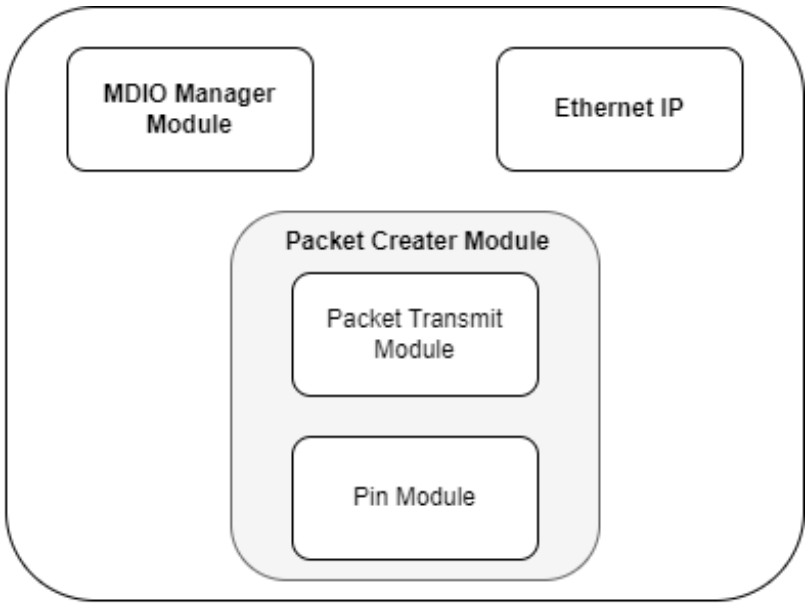

Figure 35: FPGA TX top level diagram

The MDIO Manager Module was created to write and read address and data information to the registers of Ethernet IP. It waits for request while performing write and read operations. It also allows communication between the physical layer (PHY) and the MAC layer for tasks such as monitoring status, and controlling various PHY functions. MDIO provides a standardized way for the MAC layer to control and configure the PHY devices in the network. This allows for interoperability between different types of PHYs and MACs, making it easier to upgrade or replace components in the network. The use of MDIO also enables advanced features such as energy-saving modes and link-partner auto-negotiation, which are important for optimizing network performance and reducing power consumption. Fig. 36 shows the connection of the PHY controlled by the MDIO manager with the FPGA.

Packet Creator Module consists of 2 submodules. The Pin Submodule handles precise pulse generation operations while the Packet Transmit Submodule is used to enable switching between different modes of operation. In Alignment Mode, the outputs from the Pin Module are 5 MHz signals for data channels and 1 MHz signals

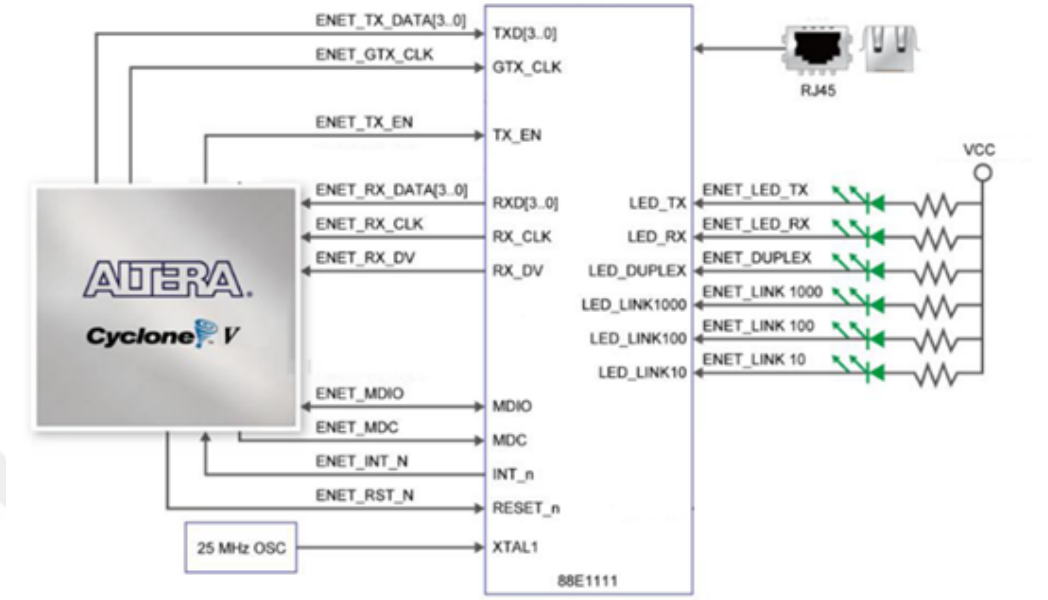

Figure 36: Ethernet PHY – FPGA connections

for synchronization channels. In QKD mode, the channel information from the Ethernet is written to the FIFO in the Pin Module. Subsequently, a message is sent to the OBC via the Ethernet with the Packet Transmit Module. When a Ping Mode request is received from the Ethernet, the Packet Transmit Module pings the OBC over Ethernet in 200ms. Subsequently, the Packet Transmit Module generates the data package for transmission.

As illustrated in Fig. 36, the receiver includes Ethernet IP, MDIO manager and Packer Create Module blocks. The MDIO manager and Ethernet IP used in the receiver are the same as the IPs used in the transmitter. The Ethernet Command Capture module receives the mode information from the Ethernet. If Alignment mode is selected, data from 4 channels is counted every 100 ms. The 1 MHz signal coming from the synchronization channel is counted to start recording the data and to ensure synchronization. In QKD mode, incoming data is written to FIFOs. The process of writing to FIFO continues as long as the signal comes from the synchronization channel. Data written to FIFO are recorded with the time they arrive. The RX

design operates at twice the speed of the TX design. This causes some data not to be captured. Synchronization is required when a signal is transferred between circuits in unrelated or asynchronous clock domains. A signal that is asynchronous with the clock is captured by passing it through Flip-Flops and ensuring its synchronization. After the captured data is saved in FIFO, it is packaged in the Packet Transmit Module and sent to the computer. Mode information can be checked during operation. When ping mode comes, Packet Transmit Module sends a packet to a computer in 200 ms.

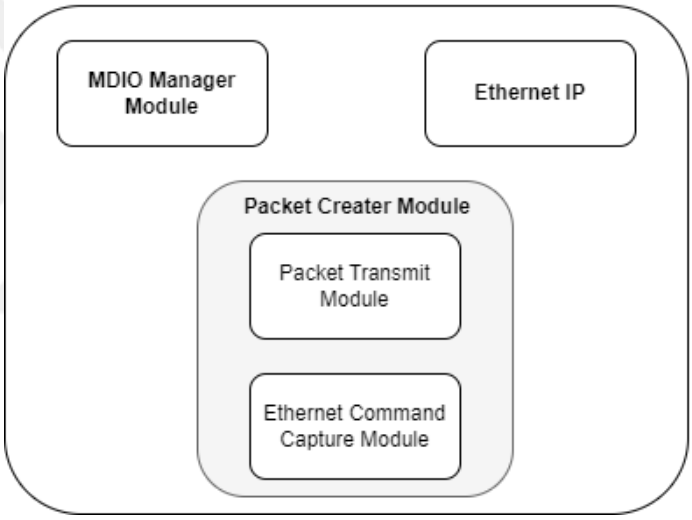

Figure 37: FPGA RX top level diagram

The Alice transfers channel information to FPGA using UDP protocol. The Alice's FPGA has a state machine that decodes the UDP packet. First it confirms that the received UDP packet is a valid channel information data packet. The data loader state machine takes the payload part of the UDP packet and redirects it to buffering module. The buffering module fills all block RAM of the Cyclone 10LP FPGA. To perform this task, the largest 16K option supported by Altera FIFO IP was used, but since there was more space, two 16K FIFOs were connected back-to-back to create a large buffer memory. The final buffer module takes 8-bit inputs and generates 2-bit laser selection output. After Alice receives transfer command from Alice OBC through

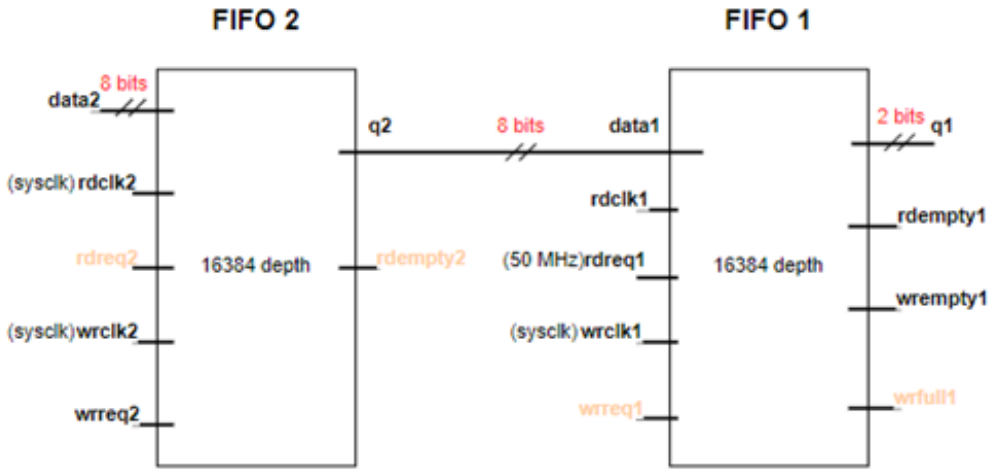

Figure 38: Back-to-Back buffering mechanism

Figure 39: Timestamp packet structure

UDP interface, Alice starts reading loaded information at FIFOs and uses output 2 bit laser selection information to generate very short electrical pulses at related channel. The implemented information loading and pulse sending mechanism lets FPGA to have deterministic pulse timing rate and simplifies overall system operation. The Fig. 38 shows the back-to-back buffering mechanism where two FIFOs are used.

At the receiver side, a 28-bit counter is used for high precision time of arrival information of the pulses received from the channels. Next to this counter, pulse channel information is added as 1 bit for each of the 4 channels. The 32 bit timestamp packet structure is presented in Fig. 39.

The functionalities implemented in FPGA design are verified in the test/development tools prior to flashing bit files to the actual FPGA board. For this purpose,

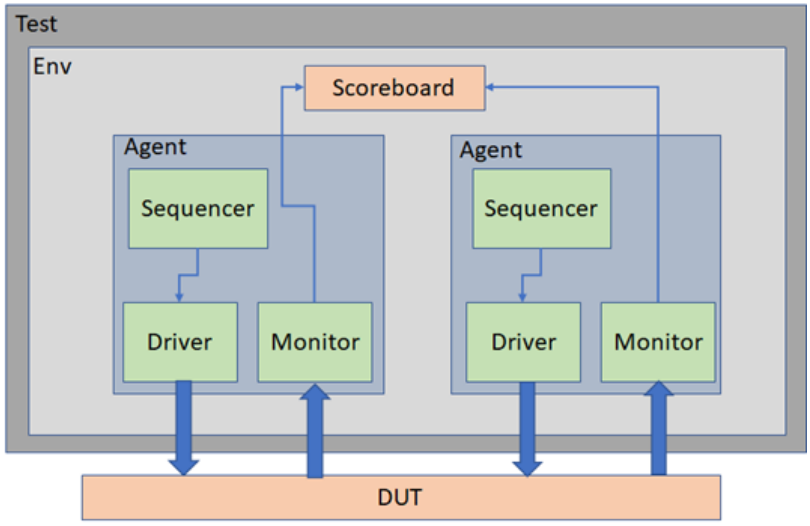

Figure 40: Verification environment

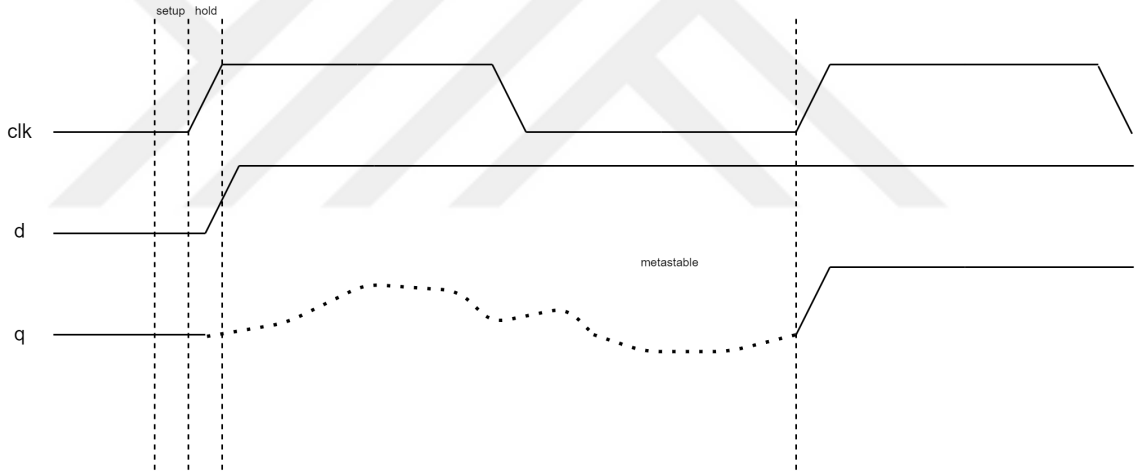

Figure 41: Sampled metastable signal

Universal Verification Methodology (UVM) infrastructure was used to verify the design in the simulation environment. Receiver and transmitter design overhead modules include Ethernet and channel signals. Two separate agents have been created in the UVM environment for Ethernet and channel signals. The Ethernet agent handles packets sent and received over Ethernet to the design. The other channel agent is designed to control the pulses to be sent to the line and to examine the pulses coming from the line. Fig. 40 shows the UVM structure created using 2 agents.

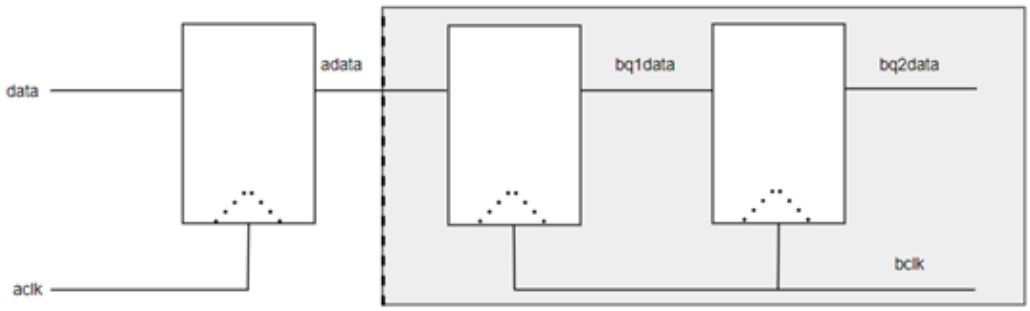

Figure 42: Inconsistency of metastable signal in circuit

3.2.2 Metastability Prevention

Metastability could pose a problem in digital circuits because it can lead to errors or malfunction. For example, if a circuit is metastable, it may produce an incorrect output value, or it may oscillate between two or more possible output values. This can cause problems in systems that rely on the accuracy of digital signals, such as computers or other digital devices. There are a number of factors that can contribute to metastability in digital circuits. One common cause is rapid transitions in the input signal, which can cause the circuit to become uncertain about the correct value. Other factors that can contribute to metastability include noise on the input or power supply, or variations in the timing or operation of the circuit. To address the problem of metastability, digital designers can use a variety of techniques, such as glitch filters, debouncing circuits, and specialized circuit designs. In addition, it may be necessary to use synchronization techniques, such as phase-locked loops, to ensure that the circuit is able to latch the correct value. In the Fig. 44, it is seen that the clock in the receiving system is asynchronous with the data in the sending system. Therefore, a metastable signal is sampled when the data changes in the setup-hold time interval of the receiving system. This will cause the remaining logic of the system to work inconsistently. If the period of the metastable signal leaving the sending system is shorter than the period of the clock of the receiving system, it is also possible that

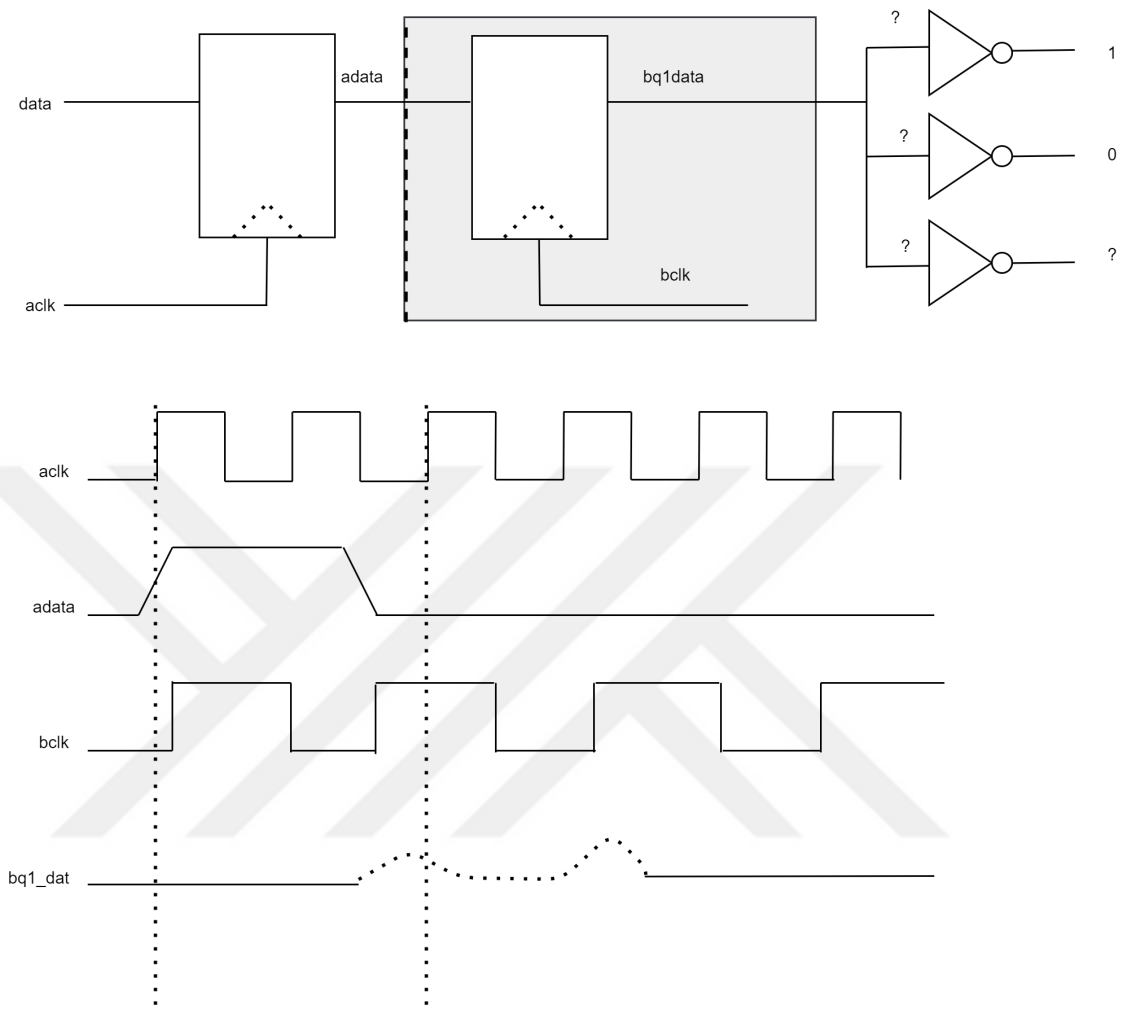

Figure 43: Metastability master-slave register solution

the relevant data is not sampled at all during the sampling period. In the Fig. 44, the clock period of the transmitter is lower than that of the receiver. When a metastable signal is given to the back of the circuit, it may cause different results in each logic. This situation is shown in the NOT Gates in the Fig. 43. Even if the same metastable signal comes to the inputs of NOT Gates, it can cause each NOT Gate to produce a different output value.

One way to mitigate the effects of metastability in a digital circuit is to use a "master-slave" flip-flop. This type of circuit uses two flip-flops connected in series, with the output of the first flip-flop (the "master") driving the input of the second

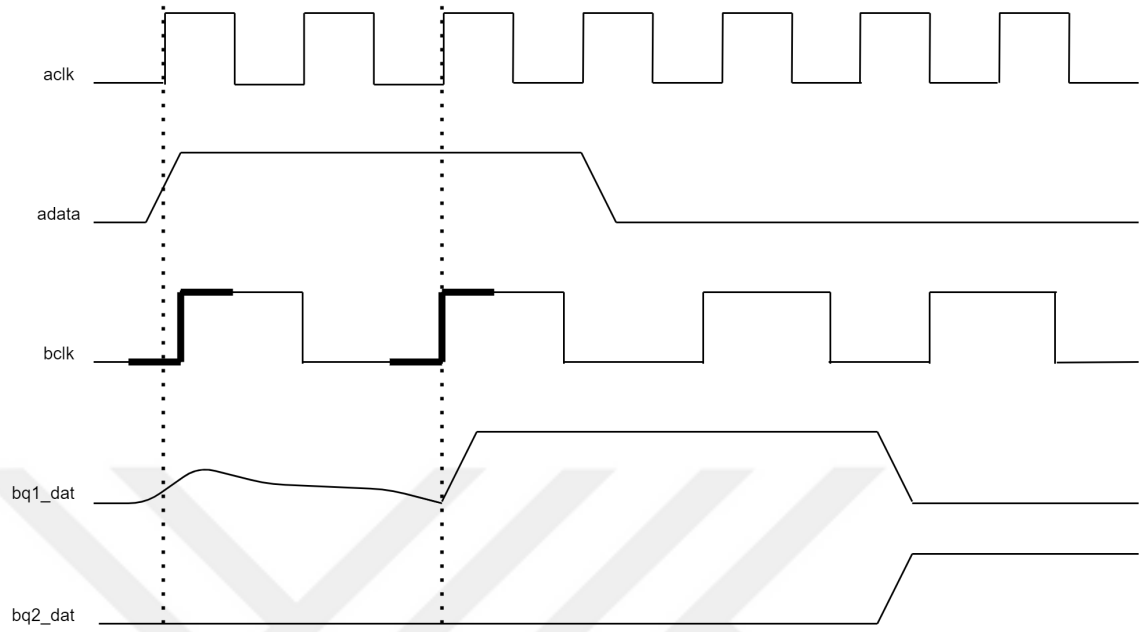

Figure 44: Stable signal capturing

flip-flop (the "slave"). The key feature of a master-slave flip-flop is that the slave flip-flop is only allowed to update its output value on the rising edge of the clock signal. This means that the slave flip-flop will only change its output value when the clock signal is stable, rather than while it is transitioning. As a result, the master-slave flip-flop is less prone to metastability than a simple flip-flop circuit. To use a master-slave flip-flop in a circuit, the input value is applied to the master flip-flop, and the output of the slave flip-flop is used as the circuit's output. The rising edge of the clock signal is used to latch the value from the master flip-flop into the slave flip-flop. This ensures that the output of the circuit remains stable, even if the input value is changing rapidly or is uncertain. Fig. 43 shows the metastability elimination solution set up using two flip flops.

In a master-slave flip-flop, it is possible for the master flip-flop to become metastable, while the slave flip-flop remains stable. This can happen if the input value to the master flip-flop changes while the clock signal is transitioning. If the master flip-flop

becomes metastable, it will be unable to decide between the two possible output values. However, the slave flip-flop will only update its output value on the rising edge of the clock signal, when the clock signal is stable. As a result, the slave flip-flop will not be affected by the metastability of the master flip-flop, and will continue to produce a stable output. In this situation, the output of the master-slave flip-flop may be delayed slightly, as the slave flip-flop will not update its output until the next rising edge of the clock signal. However, the output will still be stable and correct, even if the input value is uncertain or changing rapidly. Fig. 44 illustrates the metastability-eliminated signals are seen using two flip flops. While there is a metastable signal in the first flip flop, the problem in its transfer to the second is eliminated.

CHAPTER IV

EXPERIMENTS AND RESULTS

4.1 Photon Statistics Measurement

The ability to generate single photons is performed by analysing measured photon counts using photon statistics measurements. To validate our system we have build up the setup illustrated in Fig. 45. The 4 Laser Sources, Polarizing Beam Splitters and 50:50 Beam Splitters used in system to generate and combine 4 different polarization states to single path. The initial rough power adjustment done by Laser Sources using software, then the fixed attenuation applied on combined laser path by NDF. The fine adjustment of output power done by LND Filters. The lasers are triggered via Square signal generator and one synchronization signal provided to Time Tag Machine to synchronise measurements and transmissions, by doing that we can easily match transmitted and measured photons. At the receiver side to see effect of Dichroic Mirror as well we have used that as a reflector after NDF. The beams are splitted to two paths using 50:50 BS. To couple incoming beams to SPDs we have used aspheric lenses.

To perform photon statistics measurements we have applied 1MHz signal with duty cycle of 5% (in other words 1000ns period and pulse width is 50ns). Prior to photon statistics measurement characterization of setup is done by taking measurement snapshots along the path where laser beams are traveling until it reaches SPD1 and SPD2 detectors. The measurements are recorded by optical power meter.System analysis performed step by step, first measurements taken just after Laser Sources to analyze imperfections on the source, second measurements taken after PBS1 and PBS2, third measurements taken after BS1, fourth measurements taken after LND

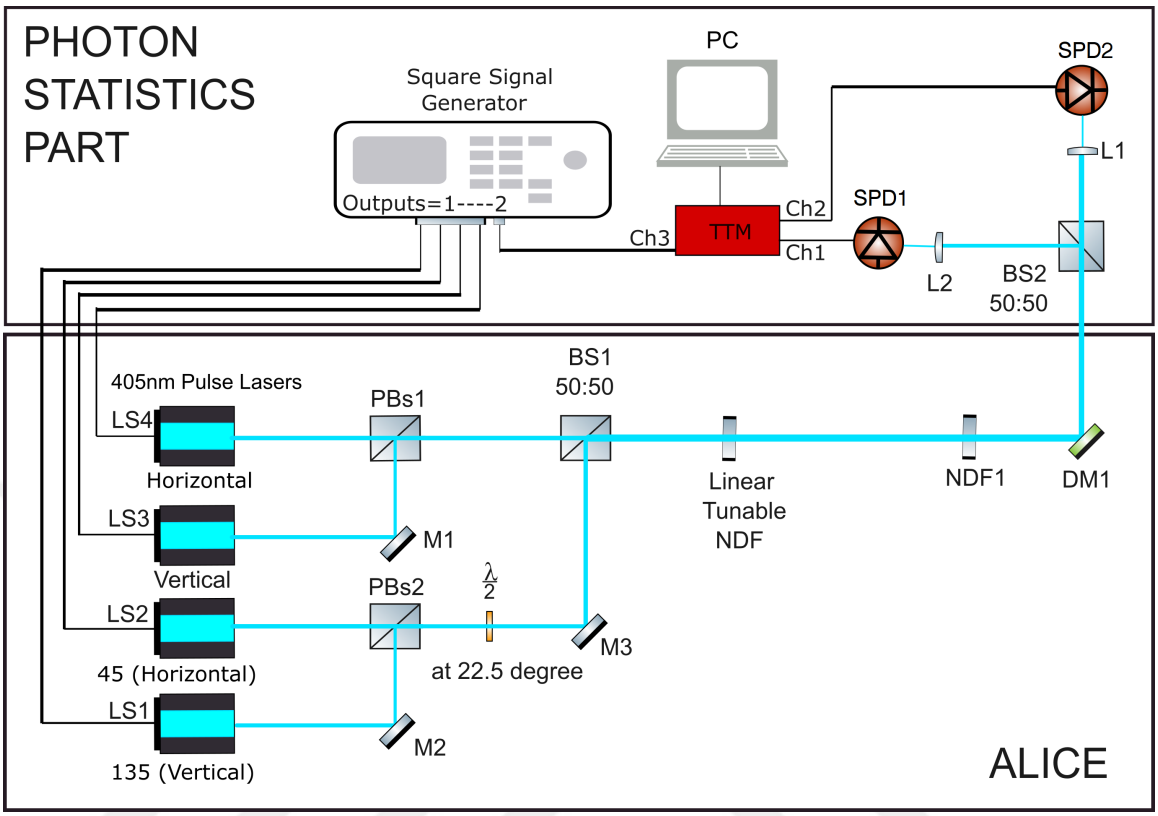

Figure 45: Schematic representation of optical setup for photon statistics

filter, fifth measurements taken at BS2.

The laser sources are coarsely tuned to get have similar output powers, the measurements of laser sources can be seen at Fig. 46. The total power fluctuations of lasers are less than 1% in 10 seconds of measurements. Since we will generate output single photons by attenuation the chance of having 2 photons by attenuation is less than 1%.

As all other optical components PBS's are also not ideal their performance is mentioned with Polarization Extinction Ratio. The PBS's that we use has Polarization Extinction Ratio of 500:1>Tp:Ts and Tp and Rs is 95% and 99% respectively. For an ideal PBS these values considered as 100%, but in reality these imperfections increases chance of reflecting or transmitting photons to paths which they shouldn't be. All though these values can be adjusted at Transmitter Side, it directly effects receiver performance thus it increases number of wrong measurements and minimum

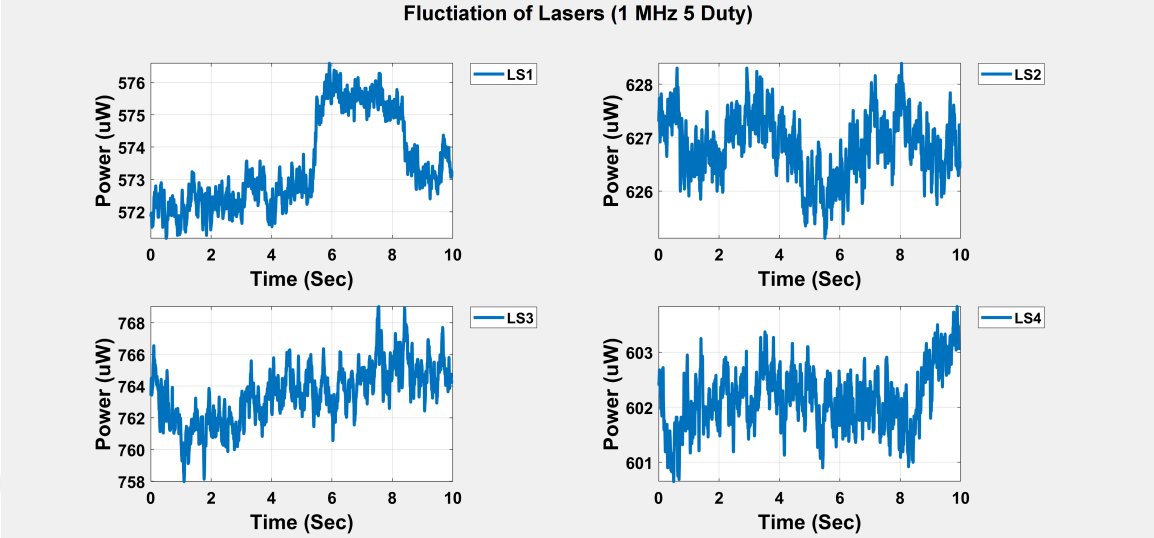

Figure 46: Fluctuations of lasers intensity

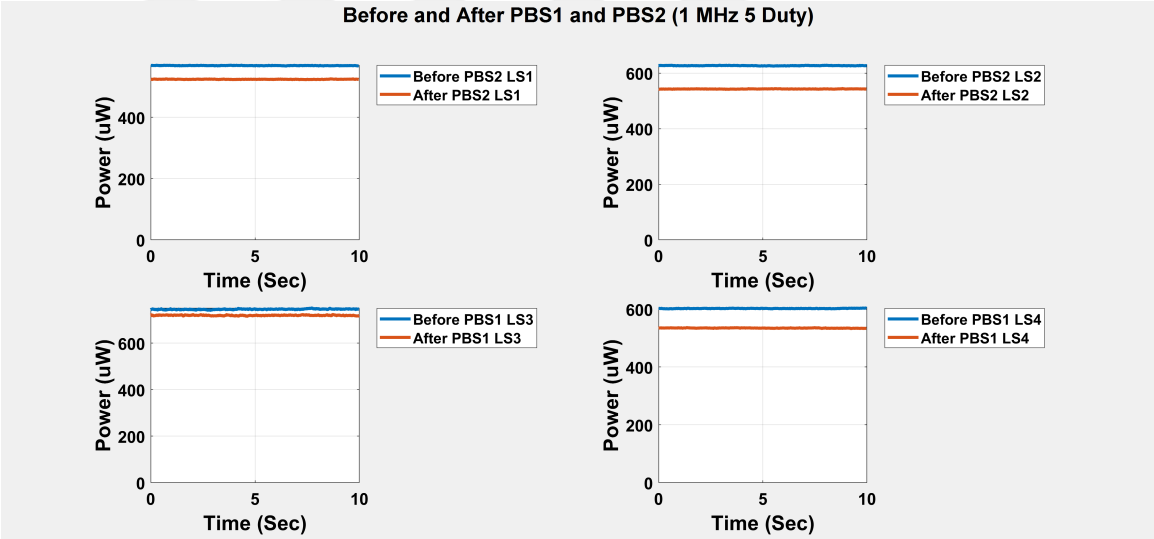

Figure 47: Characterisation of PBS

achievable QBER in system in inverse proportionally. The measurements recorded for each beam before and after PBS can be seen in at Fig. 47. As it can be also seen in the measurements, the transmit paths always had a lower amount of decrease on transmitted paths than reflected paths.

All of the beams combined using BS1 to same path. Since it is 50:50 beam splitter it is expected to have ideal reduction of all laser powers by half, but due to imperfections presented in "Verification of Optical Components" section there is

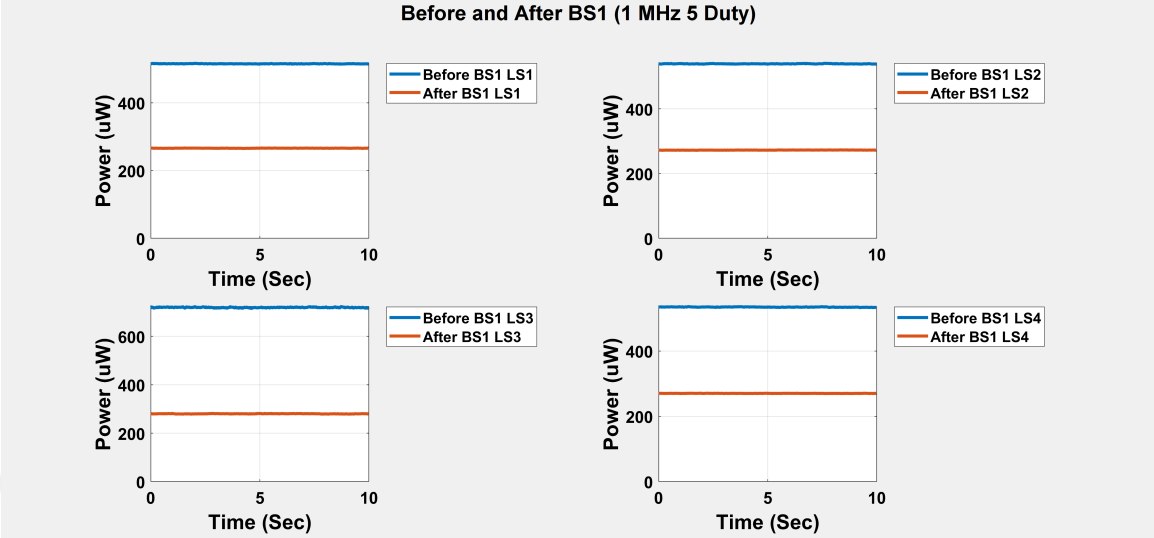

Figure 48: Characterisation of BS

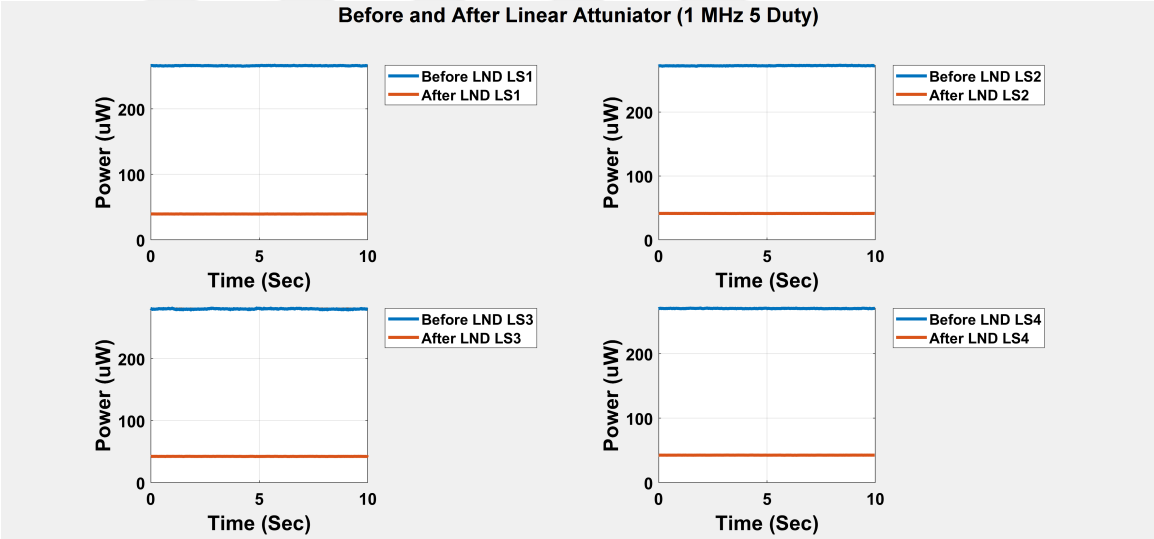

Figure 49: Characterisation of LND filters

slight polarization dependency on amount of losses. As it can be seen from Fig. 48 the amount of power measured reduced to half nearly on all Polarization States, but LS3 due to imperfections can be seen at Fig. 5.

The LND filters are generally insensitive to incoming polarizations which can be confirmed by measurements provided in Fig. 49 .All of the measured powers are equalized at LND filter by further optimization of power setting of Laser Sources.

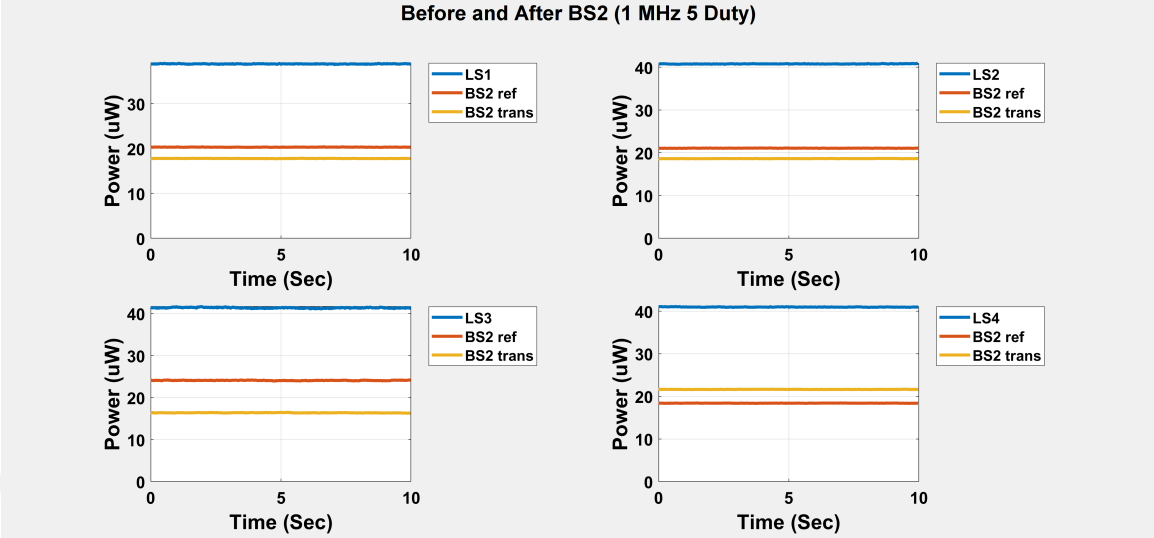

Figure 50: Characterisation of BS2

In our system diagram provided above, BS2 is considered as first splitter of receiver. In Fig. 50 polarization dependent transmission and reflections are shown for BS2 which is placed at receiver. As it is mentioned earlier the LS3(Horizontal Polarization) has the most difference between reflected and transmitted paths due to its diagonal polarization. As a result of this measurement it is expected during single photon detection measurements of LS3 path is not going to split transmitted lasers equally to detectors. Which will result different photon count rates on each detector.

Measurements are taken from SPD1 and SPD2 using the system diagram shared at Fig. 45. The tests are carried out at a repetition frequency of 1Mhz and around 50nsec. The pulse width of 50nsec selected to be close, to dead time of SPDs used in system. Using this method we have mitigated some of the possible false measurements due to environmental light might come between consecutive measurements.

In Fig. 51 the Y-axis of the graph is the number of photon measurements. Each bin at Y-axis shows photon counts at that time window. The X-axis of the graph is the time when measurement has been recorded. As it can be seen from the system diagram provided at Fig. 45 one of the signal port is provided also to time tag machine along with the SPD outputs. In the graphs we will provide the pulse recordings from

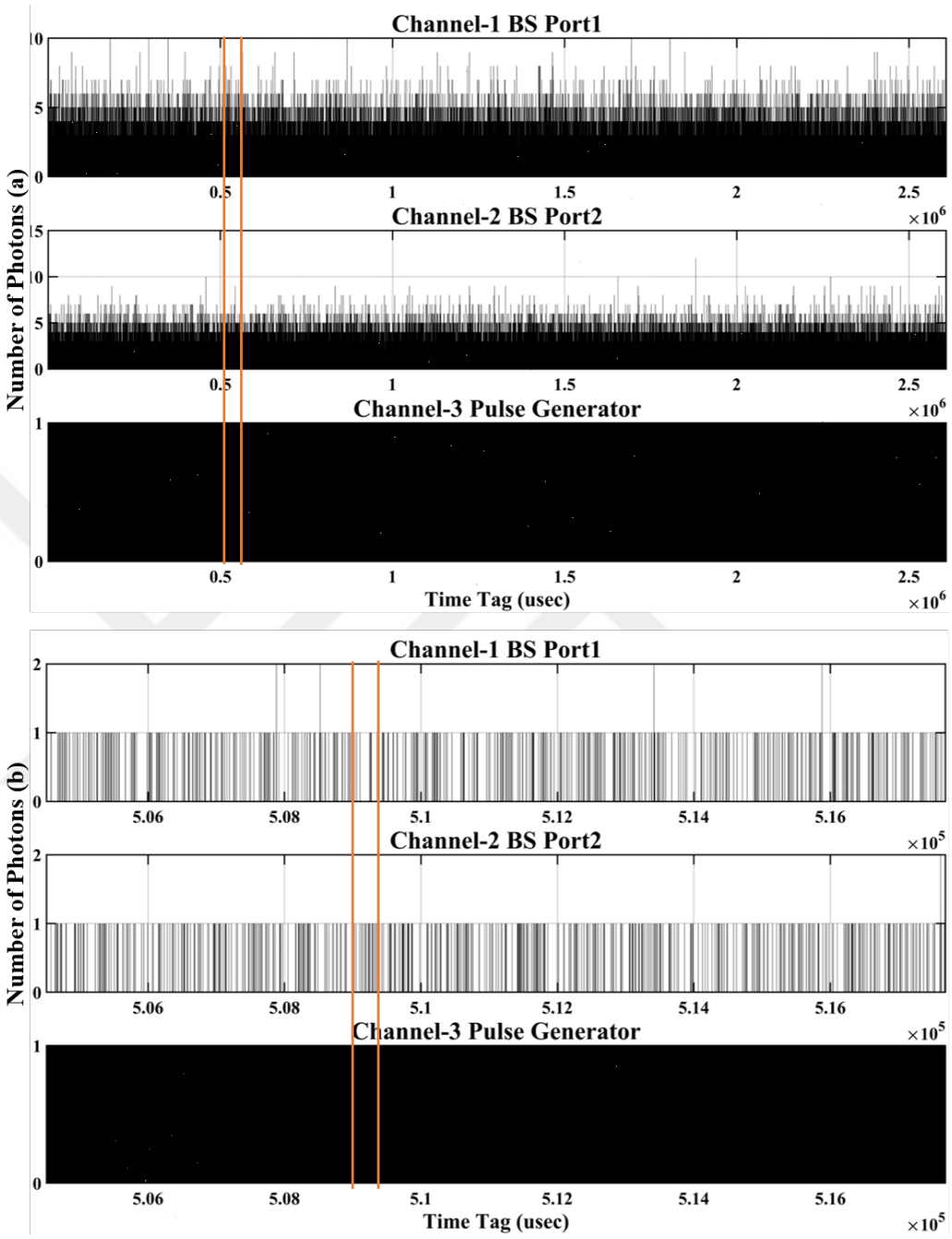

Figure 51: Measurement snapshot from time tag machine

pulse generator also shared along with SPDs to side by side comparison to match measurements. The Fig. 51.a shows full measurement and orange lines provided the reference for the zoomed data in Fig. 51.b. The measurement snapshots can be seen in more detail.

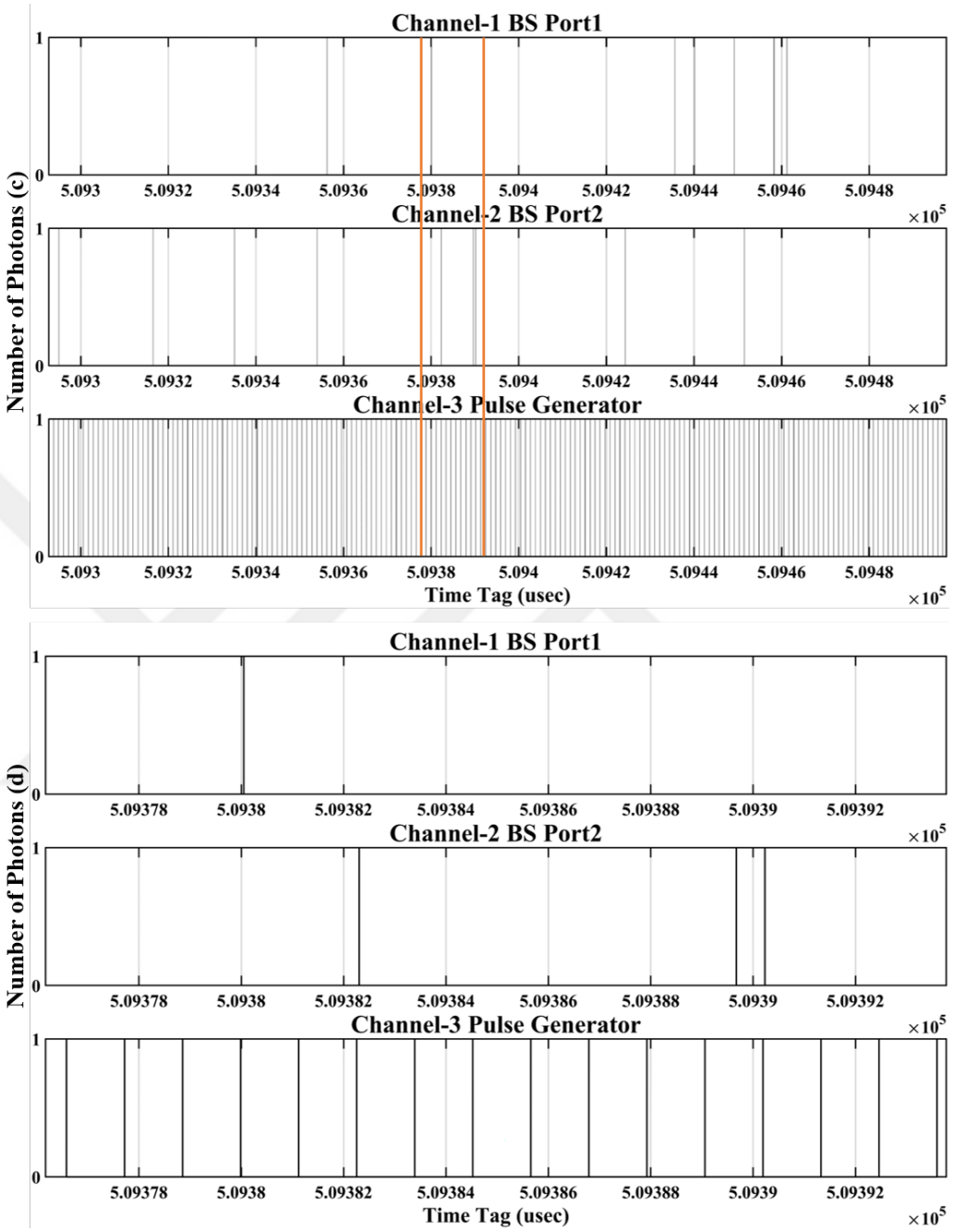

Figure 52: Zoomed to measurement snapshot

Fig. 52 is the continuation of zooming to data shared in Fig. 51. One of the most fundamental observation on measurement results is minimizing the coincidences of measurements by rough attenuation of transmitter, since a photon can not be at both transmit and reflect parts of BS it means the system has excessive amount of photons.

From Fig. 52.d Channel-1 BS Port1 and Channel-2 BS Port2 measurements it can be verified that there are no coincidences occurred during transmission. By applying this observation on measurement results we can confirm that system is operating in single photon level, otherwise we could see more photons generated in system and we should have seen much high amount of coincidences. In the measurements it can be seen that we have recorded just 1 measurements out of 10 laser pulses.

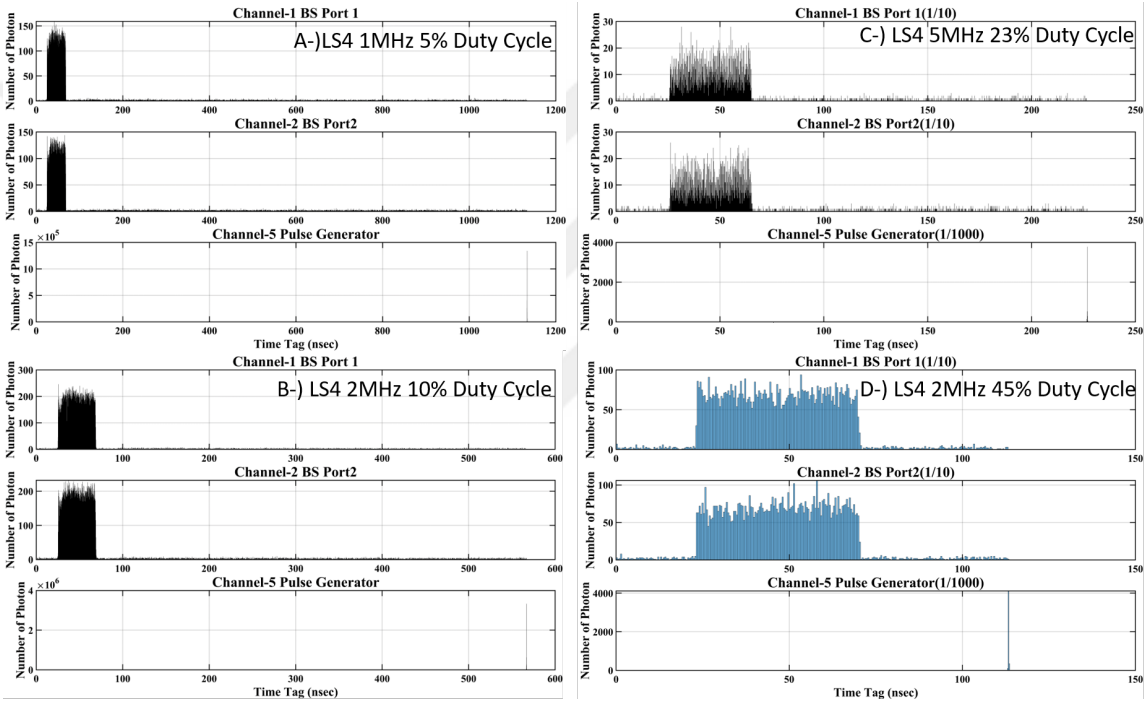

Figure 53: Overleap of measurements

To make further analysis of measurements we have created overleap of measurements by taking mod of the measurements. We have conducted this test for various frequencies and duty cycles. The dense areas on Fig. 53 is directly caused by the pulse duration of the system. The rest of the counts measure are false measurements darkcounts/background light noise combined, but all of these false measurements occured out of the actual measurement area can be neglected by help of synchronisation pulses.

In order to find the number of photons per pulse per second, it is sufficient to

know the pulse width duration generated by the laser and the number of photons measured along with the Quantum Efficiency of the detectors used in the system. From Fig. 54 the measurement snapshots of each laser can be seen. By summing all counts in Channel-1 and Channel-2 and dividing resulting number by number of pulses generated in system we can have average measurements per pulse. To have photon per pulse value we need to include quantum detection efficiency of our SPDs to calculation. By dividing average measurements recorded per pulse with the quantum efficiency of the detectors which is 18 percent for 405nm for our detectors. By applying this calculation on our system we have achieved μ value less than 0.1. Which also statistically verified that system is operating at single photon level.

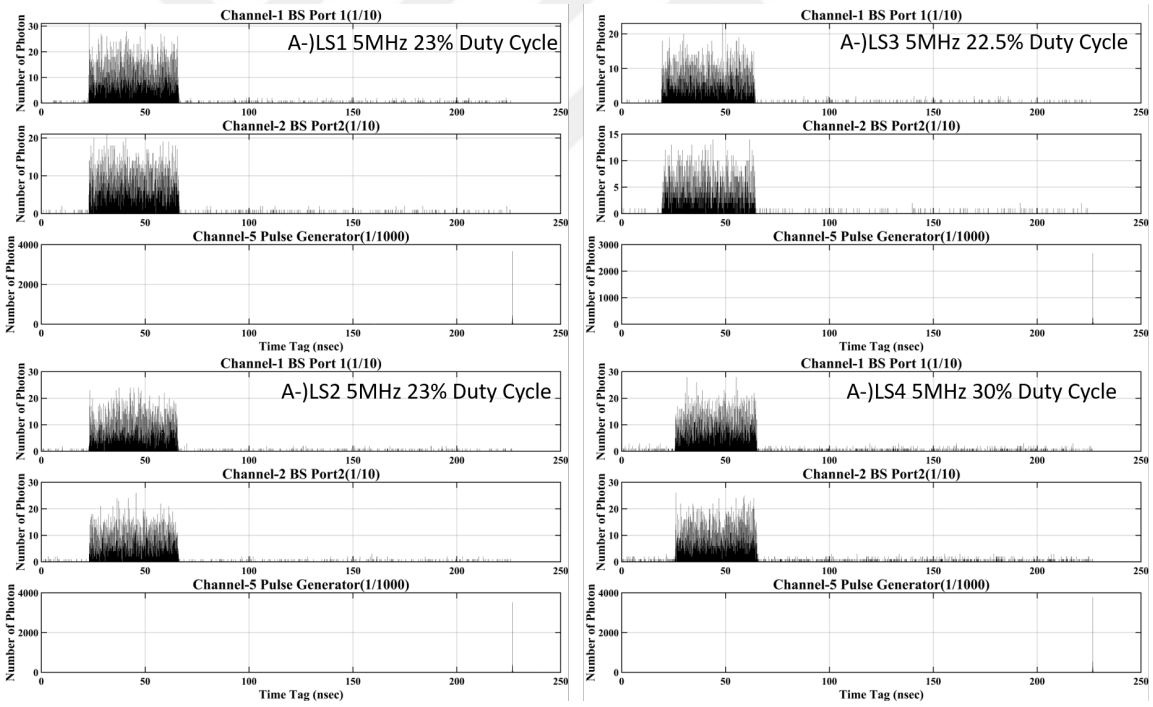

Figure 54: Zoomed to measurement snapshot

4.2 Implementation of B92 QKD System in Lab Environment

The purpose of this experiment is to verify the sub components used in system are capable of generating quantum key in lab environment prior to original target of full

scale implementation of BB84 protocol. In addition, wrong and correct measurements will be determined from the results of the experiments,by offline processing the data obtained we will generate QBER and maximum achievable secure key rate using this system. The photons are generated by turning on one of the two lasers each time in sequential order. The B92 protocol is invented by Charles Bennet who is one of the creators the famous BB84 protocol [49]. The B92 protocol is rather easier to implement, because it relies on just 2 polarization states to be transmitted. As a result it can be implemented with less components. In the B92 protocol encoding states defined as non orthogonal bases. Which means if state one |0> defined as as 0 degree polarization and the other state |1> defined as 45-degrees. The main drawback of B92 protocol is system requires twice successful measurements of what BB84 protocol requires to a key with same key length.

4.2.1 Overview of Implementation

The optical setup provided in Fig. 55 represents the implementation of B92 QKD setup implementation. The transmitter node called Alice and receiver is called Bob. This is common naming terminology of QKD literature. Alice part is equipped with 2 lasers connected to signal generator. The output of each laser has LNDFs, than a mirror to forward the beam to PBS, and one of the beams polarization is rotated by 45 degrees via halfwave plate which is placed at 22.5 degree. The 45 degree and vertical polarization's then combined at beam 50:50 beam splitter. The big reduction on beam powers are applied on combined beams using NDF1. The DM1 and DM2 is the dichroic mirrors which the details provided in previous section. In the final PoC they are used for combining alignment and QKD beams. The receiver BPF is also provided in previous sections which passes only 405nm with the +-2nm bandpass region and blocks any other wavelengths.

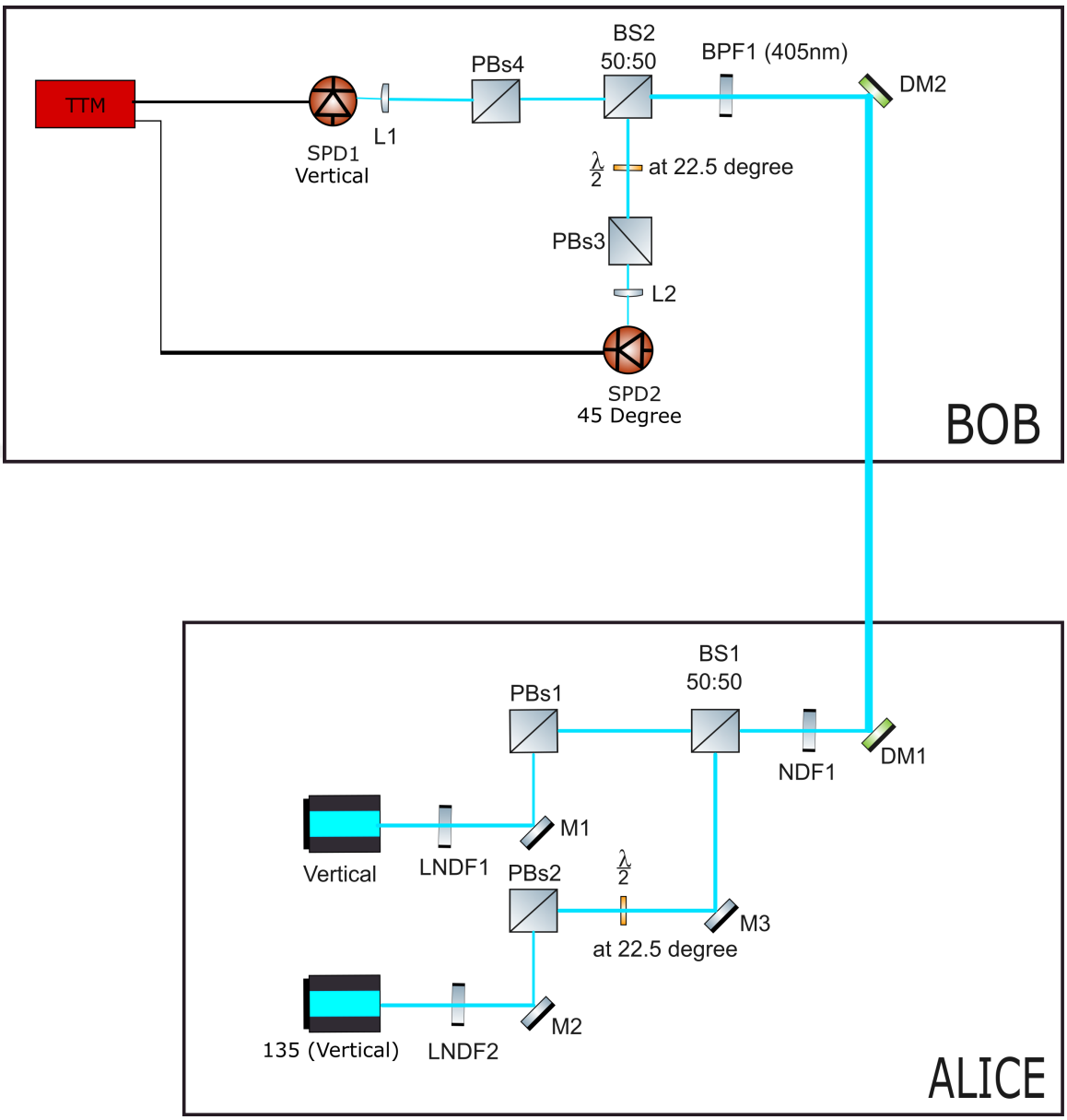

Figure 55: The schematic representation of B92 protocol based QKD setup

For example, considering that the vertically polarized photon chooses transmission port of BS, this photon exits the reflecting port of the PBS4, and it is thrown out of the system, so SPD does not make any measurement. Suppose that, the vertically polarized photon chooses reflection port of the BS. Here, the polarization direction of the photon pass through the HWP at -22.5 degrees, and HWP changes the polarization of photons to -45 degrees. Thus, the polarization of the photon becomes

45 degree. Next, there are two cases with a %50 probability for the photon from PBS3. In the first case, the photon passes through the transmission port which only horizontal polarization can pass and the photon is measured by SPD2. In the second case, it can exit from the reflection port which only the vertical polarization is reflected. In this case, the photon is removed from the system. SPD cannot measure anything. Now suppose that the photon with the other polarization direction (135 degree) comes to Bob. Again, the photon will either pass through or be reflected by %50 probability by the beam-splitter. For instance, the photon with a 45-degree polarization angle come to PBS4. In this case, that photon will encounter two situations with a %50 probability. The photon will either reflect and exit from vertical port of PBS4 or transmit and pass through the horizontal port of the system and it will be measured by the SPD1. Considering the other case, that is, the photon passes from the reflecting side of the beam splitter, located at an angle of -22.5 degrees, the HWP changes the direction of the polarization of the incident photon by 45 degrees, and the photon has a vertical polarization direction. Thus, this photon will be removed from the system and it will not be measured by SPD2. When we briefly examine the system, a vertically polarized photon can only be measured from the 135-degree port. A 45-degree photon can only be measured from the horizontal port. However, in this protocol, as can be understood from above, only %25 of the key could be measured exactly.

4.2.2 Synchronization

Synchronization is always critical in QKD systems because if the production and measurement times of the photon are known, both Alice and Bob part can create the key correctly, and also the Bob part of the system can eliminate most of the inaccurate measurements caused by the environment or SPDs. For instance, when there is no laser pulse in the system, SPDs can measure background photons. Since

the same trigger signal reaching both the time tag module and pulse laser, wrong measurements can be eliminated.

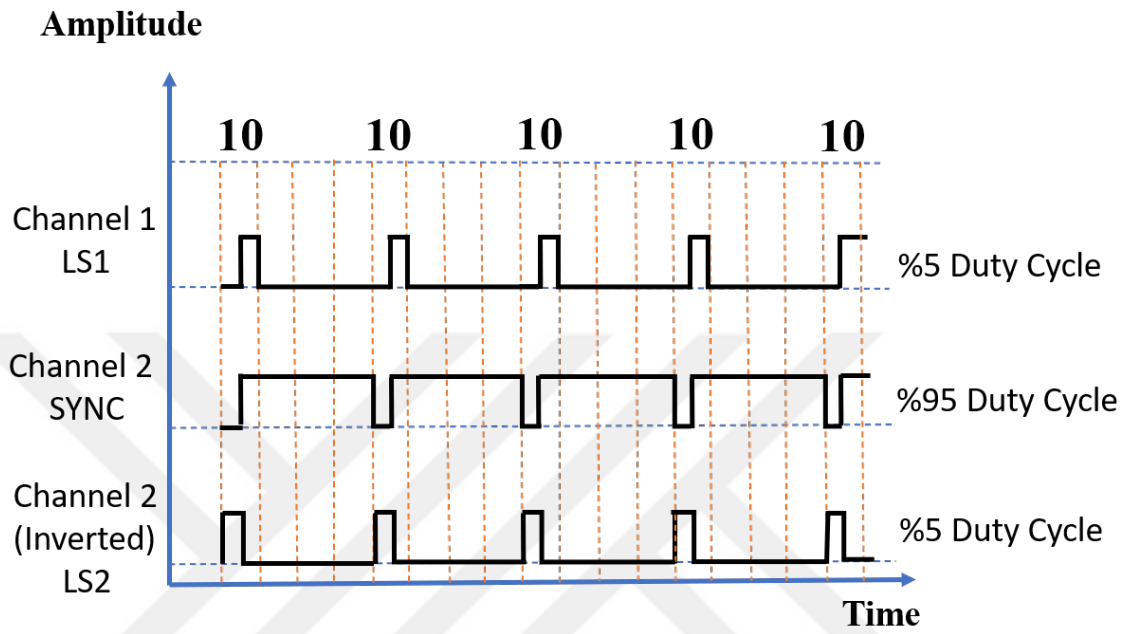

Figure 56: Synchronisation in B92 setup

When it comes to the synchronization part of the optical setup, the signals generated from the signal generator are used to drive the lasers and generate synchronization pulses. First channel of the pulse generator wired first laser (LS1) and duty cycle of the signal is %5 for 1 MHz frequency. Additionally, second channel of the signal generator wired third channel of the time tag module (TTM) and duty cycle of the signal is %95 for 1MHz square signal. This channel is used for synchronization of the system and second channel is synchronized first channel. Time tag module detects each rising edge of the pulses. Furthermore, inverted second channel wired second channel and because of inverted channel, its duty cycle becomes %5 and it is same frequency and synchronized first channel. Thus, each period two laser emit laser pulse different time and the produced key repeats periodically, so sent key looks like 1010101... Thus, each key has entered the polarization of photons. Fig. 56 is created to illustrate the generated pulse scheme. Each positive part of square wave

signal causes light emission to generate one pulse. When the square signal becomes low, laser sources do not emit light. In addition to that, the trigger signal is given to TTM, and it is used as synchronization signal. Thus, we can ignore the measurements in the region outside of this range.

The signal duration in this experiment is again selected as 1MHz repetition rate and 45 nsec pulse duration to match dead time of SPDs.

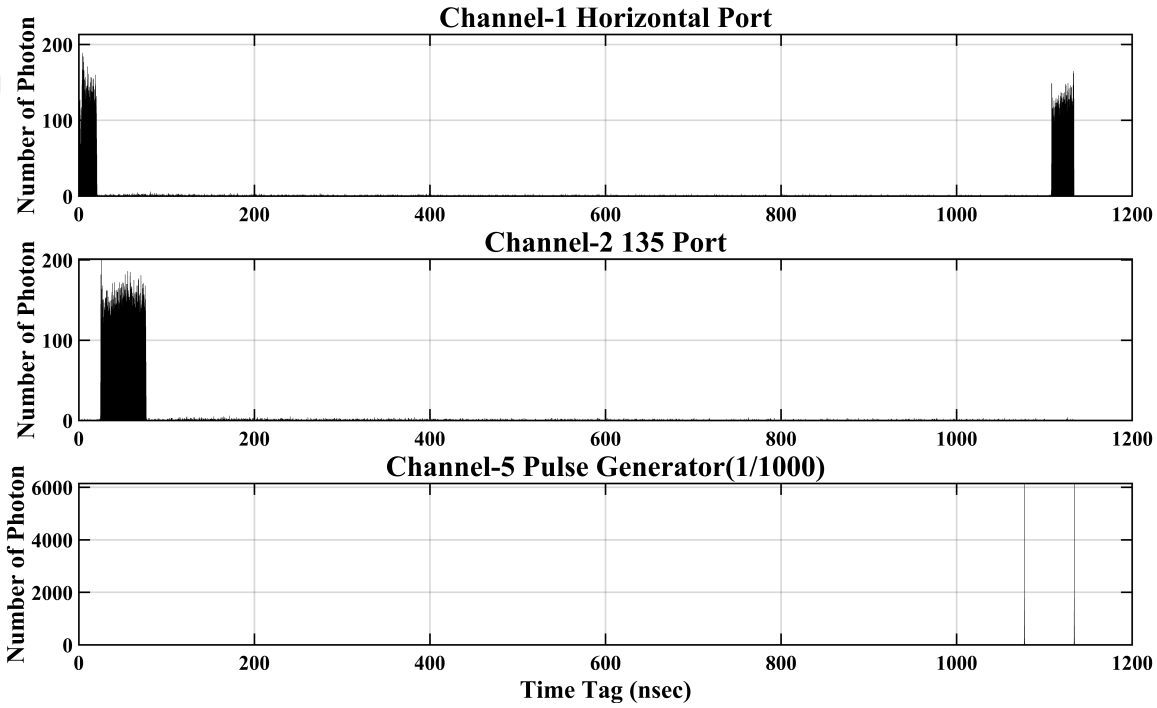

Figure 57: Measurement snapshot of B92 protocol

From Fig. 57, it is clearly seen that each laser produces photon in different time as expected. Dense part shows photon measurements. It is also seen that there is no photon measured in the system during when signal is low. Thus, it is certain that the switch is entered in the polarization of the photons in each laser signal generated. However, there is a problem at channels of TTM due to the time difference of measured photons by SPDs and measured signal, which is produced by a signal generator, by TTM. Since this delay is periodic, this delay is easily extracted from the data recorded in TTM.

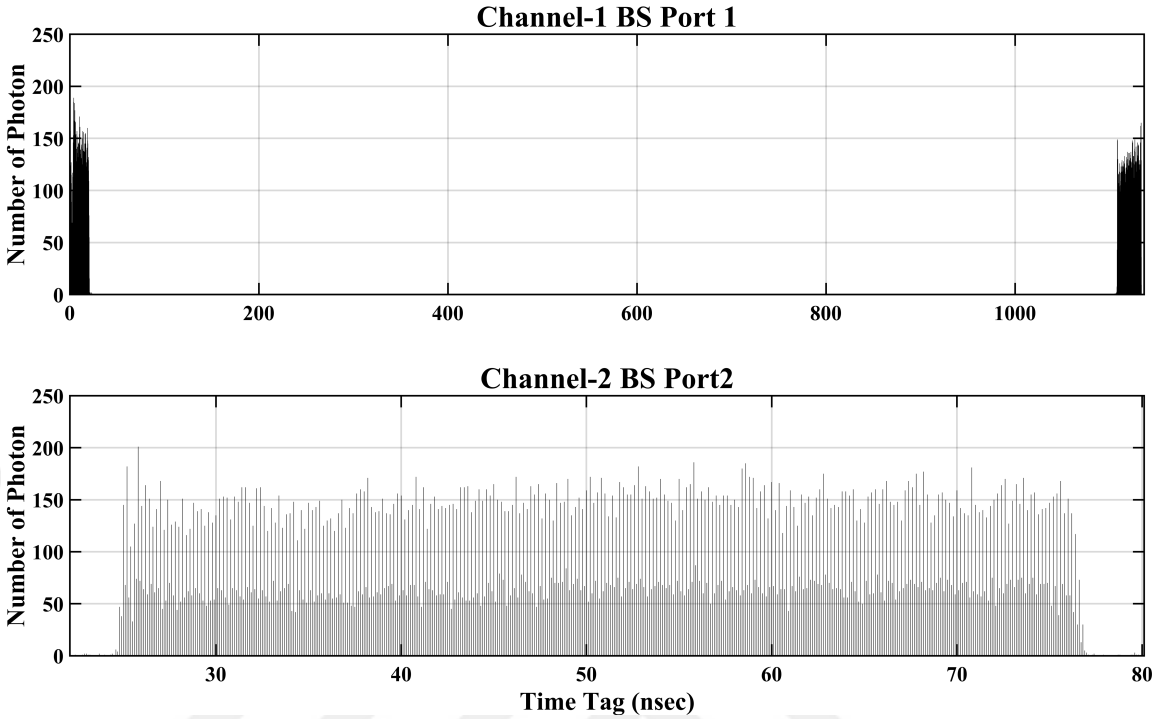

Figure 58: Measurement snapshot of B92 protocol zoomed

If each measurement from the signal generator is subtracted from the previous measurement or each measurement is started from zero-second, the measured laser photons are collected in a certain area. Thus, this range can be called the area in the system where the laser photons are located. Measurements which were made in the part outside this area are the wrong detection and the source of them are surrounding environment. Thus, these detections can be filtered out. Also, each measurement can be enumerated with this method. In Fig. 57 and Fig. 58, data is plotted with this algorithm. Laser photons and dark count measurements are easily recognized from Fig. 57. The dense part of the data is selected, Fig. 58 is obtained. It can be confirmed that this interval where many photons are arrived in short time frame is nearly equal to 45 nsec. This value is equal to the pulse width of our laser.

In order to find the number of photons per pulse per second, it is sufficient to know the pulse generated by the laser and the number of photons measured. It is also necessary to know the quantum efficiency of the detector. Moreover, all measurements

should be normalized to one second. Thus, if detections of channel-5 are counted and the total number of detection of channel-1 and channel-2 are counted and summed, the number of pulses and the number of photons are found. Then, when this rate is divided by the time passed in the total experiment, the rate for 1 second is obtained. Next, if this rate is divided by the quantum efficiency of the detectors (0.18 for 400nm). The number of photons per pulse per second of the optical system is found. Quantum efficiency is the ratio of successful detection of each photon, so the SPD can detect 18 out of 100 incoming photons. Having very low amount of coincidence(Measuring photon at multiple detectors at same time) measurements at SPDs at receiver can be used for indication of the transmitter to confirm it is operating in single photon level. The presented B92 lab setup adjusted to have mean photon number of 0.1. The offline processing measurements recorded during B92 test resulted QBER of %14 and key rate of 7.7753 KB/s.

4.3 Real time BB84 QKD System Results

After the integration and tests of sub-systems, the PoC was first tested over the air (see Fig. 59) to check its operation capability in the presence of ambient light. The QKD terminals were placed 6 meter apart from each other in LAB environment. After completing alignment of two systems in alignment mode the alignment completed. After the alignment, the QKD mode was executed and an average QBER of % 5.4 was measured with ambient light is on.

After sub-system integration and validation, the PoC was tested for underwater transmission. For this purpose, a PVC pipe filled with tap water was installed between the two terminals (Fig. 60). QBER measurements versus distance were taken and presented in Fig. 61. The rapid increase in QBER in short distances are mainly based on polarization distortion and low SNR due to imperfections associated with the thick clear glass aperture used in the implementation to withstand high pressure.

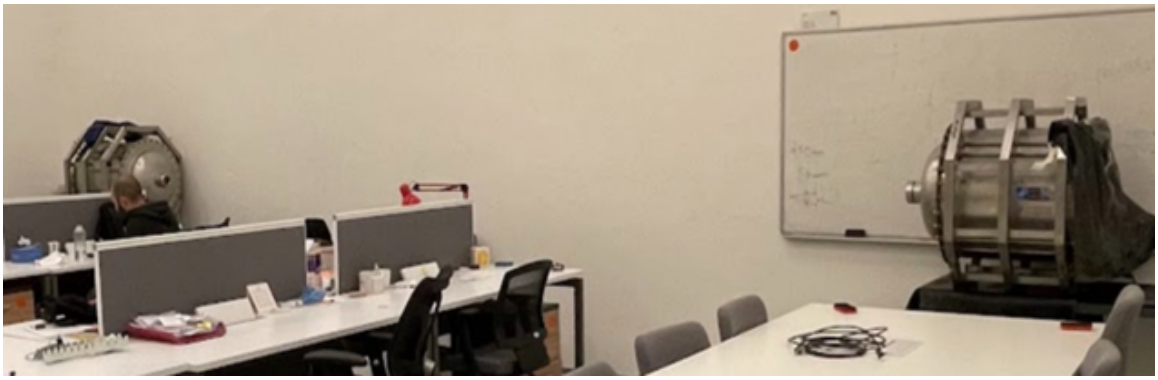

Figure 59: Over air performance tests.

Figure 60: Underwater performance tests.

A linear curve is also included in this figure via data fitting to measurement results. It exhibits a linear behaviour. An average secure key rate of about 100 qubits per second was recorded during the experiments. It is generally accepted that the BB84 protocol is secure against a sophisticated quantum attack if the QBER is less than

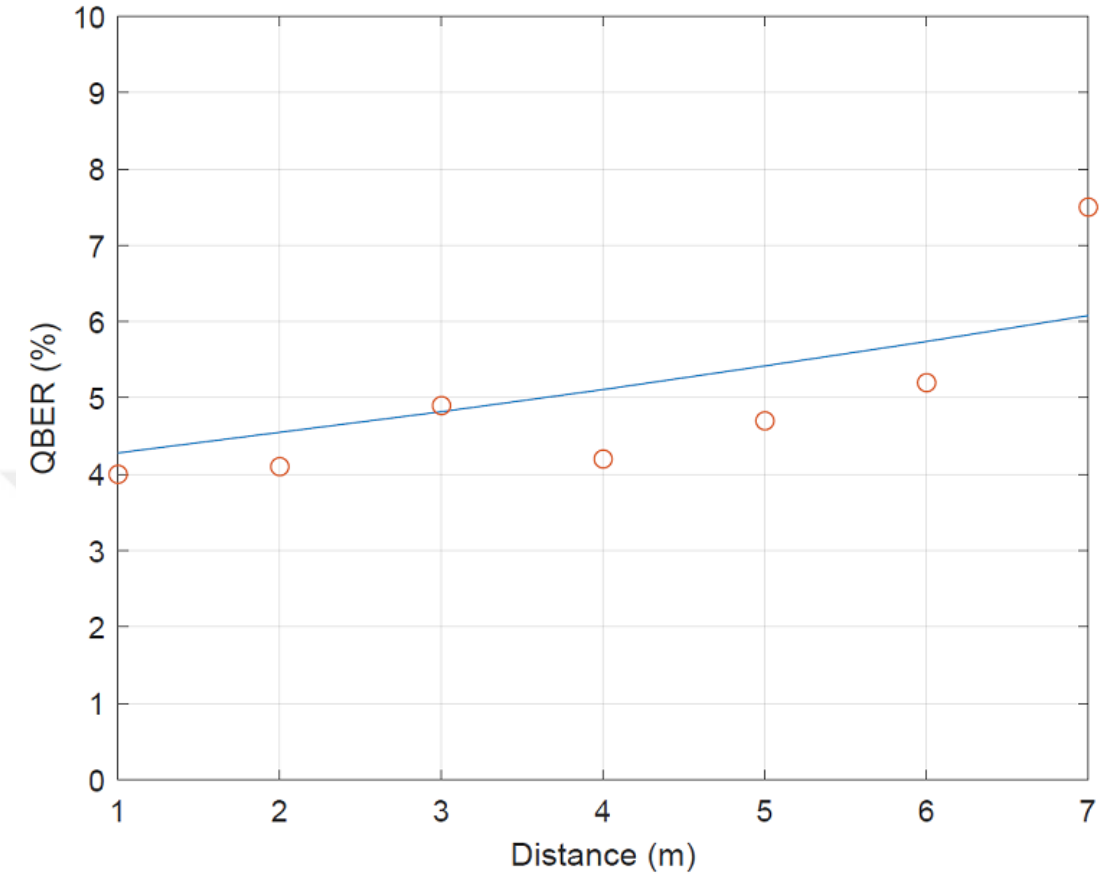

Figure 61: QBER versus distance.

0.11 [50]. It is observed that QBER safely remains below 0.11 in our implementation.

CHAPTER V

CONCLUSIONS AND FUTURE DIRECTIONS

In this thesis, we presented the implementation of a BB84-based underwater QKD system with real-time operation capability. The system was built on a hybrid computation system consisting of an FPGA and an OBC interfaced with optical front-ends. A real-time photon counting module and photon generation designs are implemented on FPGA while the rest of the QKD algorithm works on the OBC unit. The system was also equipped with a visible laser and an alignment indicator to validate successful manual alignment. The implementation of real-time QKD systems using FPGA has several challenges which we have satisfactorily addressed in our design. One of the main challenges is need for low latency operation when generating pulses and reading them from the detector. We have used digital single ended electrical interfaces to send and receive these signals. To have a cost-effective system design, we selected a basic FPGA and only used integrated block RAMs of FPGA. The total time duration of sending/receiving encoded photons is chosen to utilize all memory size of FPGA while keeping the target secure key requirements of 100 qubits per second. In real time QKD systems, the main oscillator that drives that is being used for generating photons and reading them plays critical role to know "Which state is transmitted?" and "When it is transmitted?. If the synchronisation can not be performed preferably much better than transmit pulse rate, system may not perform well and lead to higher QBER. We have observed that using the same FPGA series but different logic elements at transmit and receive side also may lead to long term stability issues due to the way IDE optimizes the implementation. Although IDE claimed that operating frequency is satisfied, shift between clocks observed at long

duration tests and lowered resulting QBER in long run tests.

By making in depth characterisation of all components and beam paths at Section II System Architecture section we have estimated maximum achievable QBER in system as 1.95 %. By checking final results in Section III we can see that minimum QBER achieved at over the air trial is 5.4% (at 6 meters) and % 5.1 (at 6 meters) at underwater signal transmission. This slight difference probably caused by more environmental light present in over air trial. The minimum QBER achieved in real time experiments seen as 4% at 1 meter which is 2% worse then best case estimated QRNG. This proves the early estimations and analysis presented at Section II can be used to estimate best case performance of real time QKD system prior to realisation of design.

This PoC system can be enhanced in several directions. In the current system, an Ethernet connection between transmitter and receiver channel serves as the public channel and Sync Cable used for syncing FPGA clocks. This can be replaced with an optical link to implement an end-to-end quantum-secure communication system demo. Such an optical link can be simultaneously used for synchronization purposes between transmitter and receiver.

The current PoC system builds upon the BB84 protocol. This protocol is commonly used in QKD systems, owing to its simplicity and effectiveness. Nonetheless, the laser sources sometimes produce pulses containing two or more photons. Thus, an eavesdropper could in principle perform a so-called Photon-Number-Splitting (PNS) attack, and obtain information about the generated key. The most common counter measure to protect QKD systems from such PNS attacks is the combination of the BB84 and the decoy-state method. The decoy-state method requires the variation of intensity during pulse generation, so as to create signal-states and decoy states. With additional upgrades on software and hardware, the developed system can be used to implement decoy-state BB84 protocol. For example, the power of each laser can be

adjusted dynamically by a software upgrade and required additional states can be obtained through this. However, the resulting delay of power adjustments using the existing RS232 connection can take up to few seconds and might be problematic for real-time implementation of decoy-state BB84. As an alternative, an electro-optical modulator (EOM) can be included prior or after the beam expander to vary the output photons dynamically in a fast manner. By applying some voltage to EOM, an additional attenuation can be employed on transmitted beam.

The key rate of the current PoC system is limited to around 100 bps which is mainly limited by the FPGA capabilities. In the current implementation, the actual time of the pulse transmission is around 9.8 msec limited by the available logic element size in the deployed FPGA. In each iteration, Alice loads 98304 samples to its FPGA and Alice waits confirmation from Bob side to start transferring the loaded pulses. It is possible to increase the generated bit sequences using a more powerful FPGA with more logic elements or OBC and FPGA can be integrated to a single SoC FPGA. Another alternative is to use a pipelined software implementation. The current version of software controls every step in separate threads and performs each operation step by step. There can be some improvements such that it pipelines multiple QKD operations and tags all of them for further processing. Another possible improvement can come from the adoption of flexible key size. The current version of implementation used a fixed length of 128 bit key in each QKD iteration. It simply discards any other measurement if the system has more measurements. It also does not process the QKD iteration if matching basis information is lower than 128 samples. The key rate can be improved by adopting a flexible key size. In such case, error correction lengths and packet sizes are required to be dynamically calculated according to the number of matching bases.

Bibliography

[1] A. Quazi and W. Konrad, "Underwater acoustic communications," *IEEE Communications Magazine*, vol. 20, no. 2, pp. 24–30, 1982.

[2] F. Mosca, G. Matte, and T. Shimura, "Low-frequency source for very long-range underwater communication," *The Journal of the Acoustical Society of America*, vol. 133, pp. EL61–EL67, 12 2012.

[3] A. Stefanov and M. Stojanovic, "Design and performance analysis of underwater acoustic networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 2012–2021, 12 2011.

[4] T. Melodia, H. Kulhandjian, L.-C. Kuo, and E. Demirors, *Advances in Underwater Acoustic Networking*, ch. 23, pp. 804–852. John Wiley & Sons Ltd, 2013.

[5] U. Lee, P. Wang, Y. Noh, L. F. M. Vieira, M. Gerla, and J.-H. Cui, "Pressure routing for underwater sensor networks," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, 2010.

[6] B. Gulbahar and O. B. Akan, "A communication theoretical modeling and analysis of underwater magneto-inductive wireless channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 9, pp. 3326–3334, 2012.

[7] M. C. Domingo, "Magnetic induction for underwater wireless communication networks," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 6, pp. 2929–2939, 2012.

[8] A. Palmeiro, M. Martín, I. Crowther, and M. Rhodes, "Underwater radio frequency communications," in *OCEANS 2011 IEEE - Spain*, pp. 1–8, 2011.

[9] J. Wang, C. Lu, S. Li, and Z. Xu, "100 m/500 mbps underwater optical wireless communication using an nrz-ook modulated 520 nm laser diode," *Opt. Express*, vol. 27, pp. 12171–12181, Apr 2019.

[10] "Sonardyne, bluecomm 200." https://www.sonardyne.com/products/bluecomm-200-wireless-underwater-link/. Accessed: 2023-07-23.

[11] J. B. Snow, J. P. Flatley, D. E. Freeman, M. A. Landry, C. E. Lindstrom, J. R. Longacre, and J. A. Schwartz, "Underwater propagation of high-data-rate laser communications pulses," in *Ocean Optics XI* (G. D. Gilbert, ed.), vol. 1750, pp. 419 – 427, International Society for Optics and Photonics, SPIE, 1992.

[12] C.-Y. Li, X.-H. Huang, H.-H. Lu, Y.-C. Huang, Q.-P. Huang, and S.-C. Tu, "A wdm pam4 fso–uwoc integrated system with a channel capacity of 100 gb/s," *Journal of Lightwave Technology*, vol. 38, no. 7, pp. 1766–1776, 2020.

[13] G. Schirripa Spagnolo, L. Cozzella, and F. Leccese, "Underwater optical wireless communications: Overview," *Sensors*, vol. 20, no. 8, p. 2261, 2020.

[14] E. Rosenkrantz and S. Arnon, *Laser Communication and Propagation through the Atmosphere and Oceans III*, vol. 9224, ch. Optimum LED wavelength for underwater optical wireless communication at turbid water, p. 922413. SPIE, 2014.

[15] G. Tuna and V. Gungor, "A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks," *International Journal of Communication Systems*, vol. 30, p. e3350, 06 2017.

[16] D. S. Terracciano, L. Bazzarello, A. Caiti, R. Costanzi, and V. Manzari, "Marine robots for underwater surveillance," *Current Robotics Reports*, vol. 1, p. 159–167, 12 2020.

[17] D. Mari, "Securing underwater wireless communication networks," *Wireless Communications, IEEE*, vol. 18, pp. 22 – 28, 03 2011.

[18] C. Bernard, P.-J. Bouvet, A. Pottier, and P. Forjonel, "Multiple access acoustic communication in underwater mobile networks," in *2021 Fifth Underwater Communications and Networking Conference (UComms)*, pp. 1–4, 2021.

[19] X. Tu, X. Xu, Z. Zou, L. Yang, and J. Wu, "Fractional fourier domain hopped communication method based on chirp modulation for underwater acoustic channels," *Journal of Systems Engineering and Electronics*, vol. 28, no. 3, pp. 449–456, 2017.

[20] A. S. M. Badrudduza, M. Ibrahim, S. M. R. Islam, M. S. Hossen, M. K. Kundu, I. S. Ansari, and H. Yu, "Security at the physical layer over gg fading and megg turbulence induced rf-uowc mixed system," *IEEE Access*, vol. 9, pp. 18123–18136, 2021.

[21] Y. Chen, M. Kong, T. Ali, J. Wang, R. Sarwar, J. Han, C. Guo, B. Sun, N. Deng, and J. Xu, "26 m/5.5 gbps air-water optical wireless communication based on an ofdm-modulated 520-nm laser diode," *Opt. Express*, vol. 25, pp. 14760–14765, Jun 2017.

[22] L.-K. Chen, Y. Shao, and Y. Di, "Underwater and water-air optical wireless communication," *J. Lightwave Technol.*, vol. 40, pp. 1440–1452, Mar 2022.

[23] A. Rukhin and J. Soto, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *National Institute of Standards and Technology (NIST)*, Apr 2010.

[24] P. Paglierani, A. H. F. Raouf, K. Pelekanakis, R. Petroccia, J. Alves, and M. Uysal, "A Primer to Underwater Quantum Key Distribution." https://10.36227/techrxiv.22299160.v2. (Online) Accessed: 2023-07-23.

[25] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 729–752, 2019.

[26] S. Loepp and W. K. Wootters, *Protecting Information: From Classical Error Correction to Quantum Cryptography*. Cambridge University Press, 2006.

[27] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, p. 16025, Nov 2016.

[28] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, p. 025002, May 2020.

[29] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of decoy state quantum key distribution over underwater turbulence channels," *Journal of the Optical Society of America B (JOSA B)*, vol. 39, no. 6, pp. 1470–1478, 2022.

[30] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5ghz repetition rate polarization-based quantum key distribution," *Applied Physics Letters*, vol. 117, no. 14, p. 144003, 2020.

[31] Z. Feng, S. Li, and Z. Xu, "Experimental underwater quantum key distribution," *Opt. Express*, vol. 29, pp. 8725–8736, Mar 2021.

[32] L. Johnson, R. Green, and M. Leeson, "A survey of channel models for underwater optical wireless communication," in *2013 2nd International Workshop on Optical Wireless Communications (IWOW)*, vol. 2, pp. 1–5, 2013.

[33] J. Sticklus, P. A. Hoeher, and R. Röttgers, "Optical underwater communication: The potential of using converted green leds in coastal waters," *IEEE Journal of Oceanic Engineering*, vol. 44, no. 2, pp. 535–547, 2019.

[34] W. Shi and M. Wang, "Characterization of particle backscattering of global highly turbid waters from viirs ocean color observations," *Journal of Geophysical Research*, vol. 122, pp. 9255–9275, 2017.

[35] S. C. Zhao, X. H. Han, Y. Xiao, Y. Shen, Y. J. Gu, and W. D. Li, "Performance of underwater quantum key distribution with polarization encoding," *J. Opt. Soc. Am. A*, vol. 36, pp. 883–892, 2019.

[36] J. Gariano and I. B. Djordjevic, "Theoretical study of a submarine to submarine quantum key distribution systems," *Opt. Express*, vol. 27, pp. 3055–3064, 2019.

[37] A. H. F. Raouf, M. Safari, and M. Uysal, "Performance analysis of quantum key distribution in underwater turbulence channels," *J. Opt. Soc. Am. B*, vol. 37, pp. 564–573, 2020.

[38] M. Lopes and N. Sarwade, "Optimized decoy state qkd for underwater free space communication," *Int. J. Quantum Inf.*, vol. 16, p. 1850019, 2018.

[39] C.-Q. Hu, Z.-Q. Yan, J. Gao, Z.-M. Li, H. Zhou, J.-P. Dou, and X.-M. Jin, "Decoy-state quantum key distribution over a long-distance high-loss air-water channel," *Phys. Rev. Appl.*, vol. 15, p. 024060, Feb 2021.

[40] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express*, vol. 26, p. 22563, 08 2018.

[41] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, and E. Karimi, "Characterization of an underwater channel for quantum communications in the ottawa river," *Opt. Express*, vol. 27, pp. 26346–26354, Sep 2019.

[42] S. Zhao, W. Li, Y. Shen, Y. Yu, X. Han, H. Zeng, M. Cai, T. Qian, S. Wang, Z. Wang, Y. Xiao, and Y. Gu, "Experimental investigation of quantum key distribution over a water channel," *Appl. Opt.*, vol. 58, pp. 3902–3907, May 2019.

[43] C.-Q. Hu, Y. Quan, J. Gao, Z. Jiao, Z.-M. Li, W.-G. Shen, Y. Chen, R.-J. Ren, L.-F. Qiao, A.-L. Yang, H. Tang, and X.-M. Jin, "Transmission of photonic polarization states through 55-m water: towards air-to-sea quantum communication," *Photonics Research*, vol. 7, p. A40, 08 2019.

[44] F. Hufnagel, A. Sit, F. Bouchard, Y. Zhang, D. England, K. Heshami, B. Sussman, and E. Karimi, "Investigation of underwater quantum channels in a 30 meter flume tank using structured photons," *New Journal of Physics*, vol. 22, p. 093074, 09 2020.

[45] S. Dong, Y. Yu, S. Zheng, Q. Zhu, L. Gai, W. Li, and Y. Gu, "Practical underwater quantum key distribution based on decoy-state bb84 protocol," *Appl. Opt.*, vol. 61, pp. 4471–4477, May 2022.

[46] J. J. Boutros and E. Soljanin, "Time-entanglement QKD: secret key rates and information reconciliation coding." https://doi.org/10.48550/arXiv.2301.00486. (Online) Accessed: 2023-07-23.

[47] a. S. G. Reed, I. S., "Polynomial codes over certain finite fields. journal of the society for industrial and applied mathematics," *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, pp. 300–304, 1960.

[48] A. Stanco, F. B. L. Santagiustina, L. Calderaro, M. Avesani, T. Bertapelle, D. Dequal, G. Vallone, and P. Villoresi, "Versatile and concurrent FPGA-based architecture for practical quantum communication systems," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–8, 2022.

[49] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, "Experimental quantum cryptography," *J. Cryptology*, vol. 5, pp. 3–28, 1992.

[50] C. Cardoso-Isidoro and F. Delgado, "Shared quantum key distribution based on asymmetric double quantum teleportation," *Symmetry*, vol. 14, no. 4, p. 713, 2022.

[51] A. Stefanov and M. Stojanovic, "Design and performance analysis of underwater acoustic networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 2012–2021, 12 2011.

VITA

Burak Kebapci studied Electrical & Electronics Engineering Major and Computer Networks Minor at the Bahcesehir University in Istanbul, Turkey between 2012 and 2015. Later on he is accepted for M.Sc degree in Electrical Electronics Engineering from Ozyegin University in 2015. At same time he joined Center of Excellence in Optical Wireless Communication Technologies (OKATEM) in 2015 as project engineer. In 2016 he became Engineering Team Lead of OKATEM. He won National Instruments Engineering Impact Award in the category of RF/Mobile Communications at 2017. The same year he graduated from M.Sc degree, he founded Hyperion Technologies and became the Chief Technology Officer (CTO) of the company. He started pursuing PhD degree in Electrical & Electronics Engineering at Ozyegin University in 2017.